Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Bengaluru 17.6.x

First Published: 2021-07-31

Last Modified: 2024-09-12

Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Bengaluru 17.6.x

Introduction to Cisco Catalyst 9800 Series Wireless Controllers

The Cisco Catalyst 9800 Series Wireless Controllers comprise next-generation wireless controllers (referred to as *controller* in this document) built for intent-based networking. The controllers use Cisco IOS XE software and integrate the radio frequency (RF) capabilities from Cisco Aironet with the intent-based networking capabilities of Cisco IOS XE to create a best-in-class wireless experience for your organization.

The controllers are enterprise ready to power your business-critical operations and transform end-customer experiences:

- The controllers come with high availability and seamless software updates that are enabled by hot and cold patching. This keeps your clients and services up and running always, both during planned and unplanned events.
- The controllers come with built-in security, including secure boot, run-time defenses, image signing, integrity verification, and hardware authenticity.
- The controllers can be deployed anywhere to enable wireless connectivity, for example, on an on-premise device, on cloud (public or private), or embedded on a Cisco Catalyst switch (for SDA deployments) or a Cisco Catalyst access point (AP).
- The controllers can be managed using Cisco Catalyst Center, programmability interfaces, for example, NETCONF and YANG,or web-based GUI or CLI.
- The controllers are built on a modular operating system. Open and programmable APIs enable the automation of your day zero to day *n* network operations. Model-driven streaming telemetry provides deep insights into your network and client health.

The controllers are available in multiple form factors to cater to your deployment options:

- Catalyst 9800 Series Wireless Controller Appliance
- Catalyst 9800 Series Wireless Controller for Cloud
- Catalyst 9800 Embedded Wireless Controller for a Cisco Switch

Note All the Cisco IOS XE programmability-related topics on the controllers are supported by DevNet, either through community-based support or through DevNet developer support. For more information, go to https://developer.cisco.com.

Note For information about the recommended Cisco IOS XE releases for Cisco Catalyst 9800 Series Wireless Controllers, see the documentation at:

https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/214749-tac-recommended-ios-xe-builds-for-wirele.html

What's New in Cisco IOS XE Bengaluru 17.6.8

There are no new features in this release.

Whats New in Cisco IOS XE Bengaluru 17.6.7

There are no new features in this release.

What's New in Cisco IOS XE Bengaluru 17.6.6a

There are no new features in this release.

This release only provides a fix for CSCwh87343: Cisco IOS XE Software Web UI Privilege Escalation Vulnerability.

For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z.

Whats New in Cisco IOS XE Bengaluru 17.6.6

There are no new features in this release.

Whats New in Cisco IOS XE Bengaluru 17.6.5

Table 1: New and Modified Software Features

Feature Name	Description and Documentation Link
Interim Accounting	From this release, the **no accounting-interim** command is supported under the policy profile to disable interim accounting. For more information, see the chapter Interim Accounting.

What's New in Cisco IOS XE Bengaluru 17.6.4

Table 2: New and Modified Software Features

Feature Name	Description and Documentation Link
Configuring the AP Console	This feature allows you to configure the AP console from the controller. The following command is introduced: • **console** For more information, see the chapter Configuring the AP Console.

Table 3: New and Modified GUI Features

Feature Name	GUI Path
Configuring the AP Console	• **Configuration > Tags & Profiles > AP Join**

What's New in Cisco IOS XE Bengaluru 17.6.3

There are no new features in this release.

What's New in Cisco IOS XE Bengaluru 17.6.2

Table 4: New and Modified Software Features

Feature Name	Description and Documentation Link
Support of 802.1X with Web Authentication on MAC Authetication Failure	Cisco IOS XE Bengaluru 17.6.2 supports 802.1X with web authentication on MAC authentication failure. For more information, see the chapter, MultipleAuthentications for a Client.
Mesh and Mesh + Flex Support for Cisco Catalyst 9124AXE Outdoor Access Points	Mesh feature and Mesh + Flex feature is supported in Cisco Catalyst 9124AXE outdoor Access Points. For more information, see the chapter Mesh Access Points.
Mesh and Mesh + Flex Support for Cisco Catalyst 9124AXI/D Outdoor Access Points	Mesh feature and Mesh + Flex feature is supported in Cisco Catalyst 9124AXI/D outdoor Access Points. For more information, see the chapter Mesh Access Points.

Feature Name	Description and Documentation Link
Per Client Bi-Directional Rate Limiting	The Per Client Bi-Directional Rate Limiting feature adds bi-directional rate limiting for each wireless clients on 802.11ac Wave 2 and 11ax APs in a Flex local switching configuration. For more information, see the chapter Quality of Service.

Table 5: New and Modified GUI Features

Feature Name	GUI Path
Per Client Bi-Directional Rate Limiting	• **Configuration > Tags & Profiles > Policy**

What's New in Cisco IOS XE Bengaluru 17.6.1

Table 6: New and Modified Software Features

Feature Name	Description and Documentation Link
Access Point Tag Persistency	From Cisco IOS XE Bengaluru 17.6.1, AP tag persistency is enabled globally on the controller. When APs join a controller with the tag persistency enabled, the mapped tags are saved on the AP without having to write the tag configurations on each AP, individually. The following command is introduced: • **ap tag persistency enable** For more information, see the chapter Access Point Tag Persistency .
AP Group NTP Server	The global NTP server configuration is replaced with per-AP group NTP server configuration. Now, you cannot configure the Cisco Hyperlocation feature without the per-AP group NTP server. The following commands are introduced: • **ntp auth-key** • **timezone delta** • **timezone use-controller** • **show ap name ntp status** • **show ap ntp status** • **show ap timezone** For more information, see the chapter Cisco Hyperlocation.

Feature Name	Description and Documentation Link
Apple Bonjour: High Availability Support for mDNS	High Availability support is now available in the mDNS feature when the controller is configured in service peer-enabled or disabled modes. For more information, see the chapter Multicast Domain Name System.
Auto-Registering Random MAC Address	If your current device is in UDN-enabled SSID, and you move to another UDN-enabled SSID, because of MAC randomization on Android, the MAC address of the device changes. The current device is then registered to the current UDN-enabled SSID using the auto-register process. The Auto-Registering Random MAC Address feature works only on Android devices versions earlier than Version 11. For more information, see the User Guide for Cisco User Defined Network Mobile Application.
Dataplane Packet Logging	Dataplane packet logging serviceability captures connectivity information related to wireless clients. Serviceability is divided into the following categories: **Global Trace Log**: Global trace logging is a mechanism to capture client connectivity , and is enabled by default. **Filtered Trace Log**: To start packet logging on a filtered trace buffer, you must enable filters using debug commands. Filters capture only the specific packet type or the packets based on the MAC address of the clients. The following commands are introduced: • **debug platform hardware chassis active qfp feature wireless datapath trace-buffer debug-level** • **debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress global-trace** • **debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress filtered-trace** • **debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject global-trace** • **debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject filtered-trace** • **clear platform hardware chassis active qfp feature wireless trace-buffer ingress filtered-trace** • **clear platform hardware chassis active qfp feature wireless trace-buffer ingress global-trace** For more information, see the chapter Dataplane Packet Logging.

Feature Name	Description and Documentation Link
Fallback for AAA Overridden VLAN	From Cisco IOS XE Bengaluru 17.6.1 onwards, fallback for AAA-overridden VLAN or VLAN groups is supported, on the policy profile. In Cisco IOS XE Bengaluru 17.5.1 Release and earlier releases, if there is a network with a single AAA server dictating policies that need to be applied to a client that may roam across different sites (having different policy definitions). If these policies are not defined on the site, the client does not get access to the network. To address this scenario, the Fallback for AAA-overridden VLAN feature is introduced. The following command is introduced: • **aaa-override vlan fallback** For more information, see the chapter WLAN Security.
FHRP Support on SDG for a Service Peer	FHRP can be enabled as SDGs and configured on the service peer. As a result, both active and standby Service Discovery Gateway's (SDGs) are available for service peers. Use the **show mdns-sd sp-sdg statistics** command to verify the details used in the Local and Wide Area Bonjour domains. For more information, see the chapter Configuring Local and Wide Area Bonjour Domains.
FQDN support for gRPC telemetry reciever	With the introduction of the FQDN Support for gRPC Subscriptions feature, along with IP addresses, FQDN can also be used for gRPC subscriptions. For more information, see the Programmability Configuration Guide, Cisco IOS XE Bengaluru 17.6.x.
Granular Reasons for Client Delete or Exclusions from SANET	Detailed or granular client deletion reason codes are available from this release for client exclusions from SANET.
Intel Analytics	Device Analtics feature is supported on Intel devices with AC9560, AC8561,AX201, AX200, AX1650, AX210, AX211, and AX1675 chipsets. Device information and other information received from the Intel devices are shared with Cisco DNA Center. This information is used to enhance device profiling on the controller. For more information, see the chapter Device Analytics.
IPv6 Ready Certification	The IPv6 feature is enhanced with the implementation of various IPv6 functionalities that are required to comply with the latest RFC specifications. For more information, see the chapter IPv6 Ready Certification.

Feature Name	Description and Documentation Link
LDAP Authentication Using sAMAccountName	LDAP authentication is enhanced to use attribute map as well, in addition to the Common Name (cn) attribute that was supported in earlier releases. Use the **show ldap server all** command to verify the attribute used for the LDAP server.
Link-Local Bridging	From Cisco IOS XE Bengaluru 17.6.1 onwards, the Link-Local Bridging feature allows you to manage link-local traffic in inter and intra controller roaming scenarios. The following command is introduced: • **link-local-bridging** For more information, see the chapter Link Local Bridging.
MAC Address Consistency	The format of the MAC addresses of some of the fields in the following CLIs are updated from *xx:xx:xx:xx:xx:xx* to *xxxx.xxxx.xxxx*. • **show ap name ble detail** • **show ap name** *ap-name* **dot11** {**5ghz** | **24ghz**} **SI device** • **show ap name** *ap-name* **dot11 5ghz slot** *slot-number* **SI device** • **show ap dot11** {**24ghz** | **5ghz**} **SI device type** • **show nmsp subscription group detail all** • **show nmsp subscription group detail ap-list**
Mesh Support for Cisco Catalyst 9124AXI/D Outdoor Access Points	Mesh feature is supported in Cisco Catalyst 9124AXI/D outdoor Access Points, with EFT quality. For queries or support on this feature, reach out to the mailer: wireless-9124-ithaca-mesh-eft-support The following commands are introduced: • **ap name mesh backhaul rate dot11abg** • **ap name mesh backhaul rate dot11ac** • **ap name name mesh backhaul rate dot11ax** • **ap name mesh backhaul rate** • **ap name mesh backhaul rate dot11n** For more information, see the chapter Mesh Access Points.

Feature Name	Description and Documentation Link
Regulatory Compliance (Rest of World) for Domain Reduction	This feature enhancement helps to reduce the number of regulatory domains by modifying the existing preprovision domain workflow to determine regulatory domain at runtime per country code. A new ROW domain is introduced and merged to include nine domains. Every AP can determine its own regulatory domain from one of the 9 domains with regulated power table and allowed radio channels. Until Cisco IOS XE Bengaluru 17.5.x, AP used the global controller country list to configure and validate all the country codes. For more information, see the chapter Regulatory Complaince Rest of the World for Domain Reduction.
Secure Boot Setup for ESXi, KVM, NFVIS, and Microsoft Hyper-V	The secure boot feature prevents malicious software applications and unauthorized operating systems from loading into the controller during the controller startup process. If the secure boot feature is enabled, only the authorized software applications boot up from the controller. For more information, see the Cisco Catalyst 9800-CL Cloud Wireless Controller Installation Guide.
Share Client Delete Reason Code at AP to the Controller	From this release, detailed or granular client deletion reason codes are transmitted from the AP to the controller. This helps the system administrators to understand the failure reason on client association while roaming or during fresh association. To find information about the client delete reasons, use the following CLIs: • **show wireless stats client delete reasons** • **show wireless stats client detail** • **show wlan name client stats**
Standby Interface Status Using Active Through SNMP	When an SNMP query is received for the standby interface information, the SNMP handlers corresponding to the CISCO-LWAPP-HA-MIB reads them from the standby interface database on the active and populates the MIB objects in the CISCO-LWAPP-HA-MIB. For more information, see the chapter Redundancy Management Interface.

Feature Name	Description and Documentation Link
Streaming Telemetry on a Cisco Catalyst 9800 Series Wireless Controller	This feature explains how to enable telemetry support for either the Wi-Fi or system health related data. Telemetry support can be enhanced up to a scale of 1000 APs and for 15000 clients. A single collector setup is used to subscribe to the requested XPaths. The telemetry feed can be used to subscribe to the data elements to monitor the APs and the clients effectively. The data is provided through the built-in Cisco wireless models. The following commands are introduced: • **gnxi (Insecure Mode)** • **gnxi (Secure Mode)** • **show gnxi state** For more information, see the chapter Streaming Telemetry on Cisco Catalyst 9800 Series Wireless Controller.
Support to Configure Radio Profile for Beam Selection for APs with C-ANT9104 Antenna and Support for Antenna Count for Cisco Catalyst 9124AXI/D Outdoor Access Points.	From Cisco IOS XE Bengaluru 17.6.1, you can configure radio profiles for the slots in the APs. You can configure radio profiles for beam-selection APs with C-ANT9104 antenna and configure antenna count for Cisco Catalyst 9124AXI/D Outdoor Access Points. You can configure the antenna beam selection for the 5-GHz slots-slot 1 and slot 2. The following commands are introduced: • **wireless profile radio** • **antenna beam-selection** • **antenna count** • **wireless tag rf** • **dot11 {24ghz | 5ghz} radio-profile** • **show wireless profile radio summary** For more information, see the chapter New Configuration Model.
Syslog Support for Advanced WIPS	This feature allows logging of alarms detected by APs in an RF environment as syslog messages in the controller. The following commands are introduced: • **awips-syslog** • **show awips syslog throttle** For more information, see the chapter Advanced WIPS.

Feature Name	Description and Documentation Link
Transport Layer Security Tunnel Support	The Transport Layer Security Tunnel (TLS) client support includes Binos processes using Linux Tun/Tap Interface. For more information, see the chapter Transport Layer Security Tunnel Support.
Wireless Management Interface	From Cisco IOS XE Bengaluru 17.6.1, Ethernet Service Port (Management Interface VRF/GigabitEthernet 0) is supported in Cisco Catalyst 9800 Series Wireless Controller. For more information, see the chapter Wireless Management Interface (WMI)
WLAN Radio Policy	The existing WLAN feature allows the broadcast of the WLAN on the specified radio on all the applicable slots. With the new radio policy feature, you can broadcast the WLAN to a corresponding slot. This option is supported only on 5-GHz band. The following command is introduced: • **radio policy dot11 5ghz slot** For more information, see the chapter WLANs.
Workgroup Bridge Support on WiFi 6 Pluggable Module for Cisco Catalyst IR1800 Rugged Series Routers	Workgroup Bridge mode support is added to the WiFi 6 Pluggable Module for Cisco Catalyst IR1800 Rugged Series Routers. For more information, see the chapter Workgroup Bridges.

Feature Name	Description and Documentation Link
Redundancy Port Interface (RIF) Manager CLIs	The following Redundancy Port Interface (RIF) manager related **show** commands are introduced: • **show platform software rif-mgr chassis active R0 resource-status** • **show platform software rif-mgr chassis standby R0 resource-status** • **show platform software rif-mgr chassis active R0 rmi-connection-details** • **show platform software rif-mgr chassis standby R0 rmi-connection-details** • **show platform software rif-mgr chassis active R0 rp-connection-details** • **show platform software rif-mgr chassis standby R0 rp-connection-details** • **show platform software rif-mgr chassis active R0 rif-stk-internal-stats** • **show platform software rif-mgr chassis standby R0 rif-stk-internal-stats** • **show platform software rif-mgr chassis active R0 lmp-statistics** • **show platform software rif-mgr chassis standby R0 lmp-statistics** • **clear platform software rif-mgr chassis active R0 clear-lmp-counters** • **clear platform software rif-mgr chassis standby R0 clear-lmp-counters**

Table 7: New and Modified GUI Features

Feature Name	GUI Path
Access Point Tag Persistency	• **Configuration > Tags & Profiles > Tags** • **Configuration** > **Wireless** > **Access Points**
Intel Analytics	• **Configuration > Tags & Profiles > WLANs** • **Monitoring > Wireless > Clients**
Link-Local Bridging	• **Configuration > Tags & Profiles > Policy**

Feature Name	GUI Path
MAC Address Consistency	• **Configuration > Security > Local Policy** • **Configuration > Tags & Profiles > AP Join** • **Configuration > Security > AAA > AAA Advanced > Device Authentication** • **Troubleshooting > Radioactive Trace** • **Configuration > Wireless > Hotspot/OpenRoaming**. • **Troubleshooting > AP Packet Capture** • **Monitoring > Wireless > Clients** • **Configuration > Wireless Setup > Basic** • **Configuration > Wireless > Mobility** • **Configuration > Tags & Profiles > Tags > AP > Static**
Mesh Support for Cisco Catalyst 9124AX Outdoor Access Points	• **Configuration > Wireless > Access Points** • **Configuration >Wireless > Mesh > Profiles**
Regulatory Compliance (Rest of World) for Domain Reduction	• **Configuration > Tags & Profiles > AP Join**
Support to Configure Radio Profile for Beam Selection for APs With C-ANT9104 Antenna and Support for Antenna Count for Cisco Catalyst 9124AX Outdoor Access Points	• **Configuration > Tags & Profiles > RF/Radio** • **Configuration > Wireless > Access Points**
WLAN Radio Policy	• **Configuration > Tags & Profiles > WLANs**
WLAN Simplification	**Configuration > Wireless Setup > WLAN Wizard**

MIBs

The following MIBs are modified:

- AIRESPACE-WIRELESS-CAPABILITY.my
- AIRESPACE-WIRELESS-MIB.my
- CISCO-LWAPP-AP-CAPABILITY.my
- CISCO-LWAPP-AP-MIB.my

- CISCO-LWAPP-CDP-CAPABILITY.my
- CISCO-LWAPP-DOT11-CAPABILITY.my
- CISCO-LWAPP-DOT11-CLIENT-CALIB-CAPABILITY.my
- CISCO-LWAPP-DOT11-CLIENT-CAPABILITY.my
- CISCO-LWAPP-DOT11-CLIENT-MIB.my
- CISCO-LWAPP-DOT11-MIB.my
- CISCO-LWAPP-DOWNLOAD-CAPABILITY.my
- CISCO-LWAPP-GUEST-LAN-CAPABILITY.my
- CISCO-LWAPP-IPV6-CAPABILITY.my
- CISCO-LWAPP-MESH-CAPABILITY.my
- CISCO-LWAPP-MESH-LINKTEST-CAPABILITY.my
- CISCO-LWAPP-MESH-MIB.my
- CISCO-LWAPP-MFP-CAPABILITY.my
- CISCO-LWAPP-MOBILITY-CAPABILITY.my
- CISCO-LWAPP-MOBILITY-EXT-CAPABILITY.my
- CISCO-LWAPP-QOS -CAPABILITY.my
- CISCO-LWAPP-QOS-MIB.my
- CISCO-LWAPP-REAP-CAPABILITY.my
- CISCO-LWAPP-RF-CAPABILITY.my
- CISCO-LWAPP-RF-MIB.my
- CISCO-LWAPP-ROGUE-CAPABILITY.my
- CISCO-LWAPP-ROGUE-MIB.my
- CISCO-LWAPP-RRM-CAPABILITY.my
- CISCO-LWAPP-RRM-MIB.my
- CISCO-LWAPP-SI-CAPABILITY.my
- CISCO-LWAPP-TC-MIB.my
- CISCO-LWAPP-TUNNEL-CAPABILITY.my
- CISCO-LWAPP-WLAN-CAPABILITY.my
- CISCO-LWAPP-WLAN-MIB.my
- CISCO-LWAPP-WLAN-POLICY-CAPABILITY.my
- CISCO-LWAPP-WLAN-SECURITY-CAPABILITY.my
- CISCO-WIRELESS-HOTSPOT-CAPABILITY.my

Behavior Change

- Two ciphers named *3des-ede-cbc-sha* and *ecdhe-rsa-3des-ede-cbc-sha* are removed from the following CLIs:
  - **ip http client secure-ciphersuite**
  - **ip http secure-ciphersuite**
- Memory utility events are not included in the AP client-trace system events.
- A new CLI named **wireless client ip-address deauthenticate** is introduced to deauthenticate wirelesss clients based on their IP address.
- A new CLI named **wireless client username deauthenticate** is introduced to deauthenticate wirelesss clients with a given username.
- The following **show** command ouputs are updated to include link-local multicast:
  - **show wireless multicast**
  - **show platform software l2m chassis active F0 global**
- A new **show ap name wlan vlan** command is introduced to display operational WLAN-VLAN mappings per AP.
- Cisco Catalyst Wi-Fi 6 (802.11ax) APs do not support Universal AP or Priming feature.
- Client MFP is supported only on Cisco Wave 1 APs and not supported on Cisco Wave 2 APs.
- Deprecated the insecure TLS version (TLSv1 and TLSv1.1) for HTTP server. The web configuration now allows only TLS protocols (TLSv1.2 and later).

Interactive Help

The Cisco Catalyst 9800 Series Wireless Controller GUI features an interactive help that walks you through the GUI and guides you through complex configurations.

You can start the interactive help in the following ways:

- By hovering your cursor over the blue flap at the right-hand corner of a window in the GUI and clicking **Interactive Help**.
- By clicking **Walk-me Thru** in the left pane of a window in the GUI.
- By clicking **Show me How** displayed in the GUI. Clicking **Show me How** triggers a specific interactive help that is relevant to the context you are in.

  For instance, **Show me How** in **Configure** > **AAA** walks you through the various steps for configuring a RADIUS server. Choose **Configuration**> **Wireless Setup** > **Advanced** and click **Show me How** to trigger the interactive help that walks you through the steps relating to various kinds of authentication.

The following features have an associated interactive help:

- Configuring AAA

- Configuring FlexConnect Authentication
- Configuring 802.1X Authentication
- Configuring Local Web Authentication
- Configuring OpenRoaming
- Configuring Mesh APs

Note If the WalkMe launcher is unavailable on Safari, modify the settings as follows:

1. Choose **Preferences** > **Privacy**.
2. In the **Website tracking** section, uncheck the **Prevent cross-site tracking** check box to disable this action.
3. In the **Cookies and website data** section, uncheck the **Block all cookies** check box to disable this action.

Important Notes

- To migrate public IP address from 16.12.x to 17.x. ensure that you configure the **service internal** command. If you do not configure the **service internal** command, the IP address does not carry forward.
- The Cisco Aironet 2800 and 3800 APs do not reset an interface (to clear any Ethernet interface physical layer issues) if the Dynamic Host Configuration Protocol (DHCP) does not resolve the IP address within a certain duration.

Supported Hardware

The following table lists the supported virtual and hardware platforms. (See Table 10: Supported PIDs and Ports, on page 17 for the list of supported modules.)

Table 8: Supported Virtual and Hardware Platforms

Platform	Description
Cisco Catalyst 9800-80 Wireless Controller	A modular wireless controller with up to 100-GE modular uplinks and seamless software updates. The controller occupies 2-rack unit space and supports multiple module uplinks.
Cisco Catalyst 9800-40 Wireless Controller	A fixed wireless controller with seamless software updates for mid-size to large enterprises. The controller occupies 1-rack unit space and provides four 1-GE or 10-GE uplink ports.

Platform	Description
Cisco Catalyst 9800 Wireless Controller for Cloud	A virtual form factor of the Catalyst 9800 Wireless Controller that can be deployed in a private cloud (supports ESXi, KVM, and NFVIS on ENCS hypervisors), or in the public cloud as Infrastructure as a Service (IaaS) in Amazon Web Services (AWS) and Google Cloud Platform (GCP) marketplace.
Cisco Catalyst 9800 Embedded Wireless Controller for Switch	The Catalyst 9800 Wireless Controller software for the Cisco Catalyst 9000 switches bring the wired and wireless infrastructure together with consistent policy and management. This deployment model supports only SD Access, which is a highly secure solution for small campuses and distributed branches.
Cisco Catalyst 9800-L Wireless Controller	The Cisco Catalyst 9800-L Wireless Controller is the first low-end controller that provides a significant boost in performance and features.

The following table lists the host environments supported for private and public cloud.

Table 9: Supported Host Environments for Public and Private Cloud

Host Environment	Software Version
VMware ESXi	• VMware ESXi vSphere 6.0, 6.7, and 7.0 • VMware ESXi vCenter 6.0, 6.5, 6.7 and 7.0
KVM	• Linux KVM based on Red Hat Enterprise Linux 7.6, 7.8, and 8.2 • Linux KVM based on Red Hat Enterprise Linux 7.1 and 7.2 • Ubuntu 16.04.5 LTS, Ubuntu 18.04.5 LTS, Ubuntu 20.04.5 LTS
AWS	AWS EC2 platform
NFVIS	ENCS 3.8.1 and 3.9.1
GCP	GCP marketplace
Microsoft Hyper-V	Windows 2019 Server and Windows Server 2016 (Version 1607) with Hyper-V Manager (Version 10.0.14393)

The following table lists the supported Cisco Catalyst 9800 Series Wireless Controller hardware models.

The Base PIDs are the model numbers of the controller.

The Bundled PIDs indicate the orderable part numbers for the Base PIDs that are bundled with a particular network module. Running the **show version**, **show module** or **show inventory** command on such a controller (bundled PID) displays its Base PID.

Note that unsupported SFPs will bring down a port. Only Cisco-supported SFPs (GLC-LH-SMD and GLC-SX-MMD) should be used on the RP port of C9800-80-K9 and C9800-40-K9.

Table 10: Supported PIDs and Ports

Controller Model	Description
C9800-CL-K9	Cisco Catalyst Wireless Controller as an infrastructure for Cloud.
C9800-80-K9	Eight 1/10-Gigabit Ethernet SFP or SFP+ ports and two power supply slots. The following SFPs are supported: • GLC-BX-D • GLC-BX-U • GLC-EX-SMD • GLC-LH-SMD • GLC-SX-MMD • GLC-ZX-SMD • GLC-TE

Controller Model	Description
	The following enhanced SFPs are supported: • SFP-10G-AOC1M • SFP-10G-AOC2M • SFP-10G-AOC3M • SFP-10G-AOC5M • SFP-10G-AOC7M • SFP-10G-AOC10M • SFP-10G-SR • SFP-10G-SR-S • SFP-10G-SR-X • SFP-10G-LR • SFP-10G-LRM • SFP-10G-LR-X • SFP-10G-ER • SFP-10G-ZR • SFP-H10GB-CU1M • SFP-H10GB-CU1.5M • SFP-H10GB-CU2M • SFP-H10GB-CU2.5M • SFP-H10GB-CU3M • SFP-H10GB-CU5M • SFP-H10GB-ACU7M • SFP-H10GB-ACU10M • DWDM-SFP10G-30.33 • DWDM-SFP10G-61.41 • FINISAR-LR – FTLX1471D3BCL • FINISAR-SR – FTLX8574D3BCL [1]

Controller Model	Description
	The following QSFP+s are supported: • QSFP-40G-SR4 • QSFP-40G-LR4 • QSFP-40GE-LR4 • QSFP-40G-ER4 • QSFP-40G-SR4-S • QSFP-40G-LR4-S • QSFP-40G-SR-BD • QSFP-40G-BD-RX • QSFP-100G-SR4-S • QSFP-100G-LR4-S
C9800-40-K9	Four 1/10-Gigabit Ethernet SFP or SFP+ ports and two power supply slots The following SFPs are supported: • GLC-BX-D • GLC-BX-U • GLC-LH-SMD • GLC-SX-MMD • GLC-EX-SMD • GLC-ZX-SMD • GLC-TE

Controller Model	Description
	The following enhanced SFPs are supported: • SFP-10G-AOC1M • SFP-10G-AOC2M • SFP-10G-AOC3M • SFP-10G-AOC5M • SFP-10G-AOC7M • SFP-10G-AOC10M • SFP-10G-SR • SFP-10G-SR-S • SFP-10G-SR-X • SFP-10G-LR • SFP-10G-LRM • SFP-10G-LR-X • SFP-10G-ER • SFP-10G-ZR • SFP-H10GB-CU1M • SFP-H10GB-CU1.5M • SFP-H10GB-CU2M • SFP-H10GB-CU2.5M • SFP-H10GB-CU3M • SFP-H10GB-CU5M • SFP-H10GB-ACU7M • SFP-H10GB-ACU10M • DWDM-SFP10G-30.33 - DWDM-SFP10G-61.41 • FINISAR-LR – FTLX1471D3BCL [1] • FINISAR-SR – FTLX8574D3BCL [1]

Controller Model	Description
C9800-L-C-K9	• 4x2.5/2-Gigabit ports • 2x10/5/2.5/1-Gigabit ports The following SFPs are supported: • GLC-BX-D • GLC-BX-U • GLC-LH-SMD • GLC-SX-MMD • GLC-ZX-SMD • GLC-TE

Controller Model	Description
C9800-L-F-K9	• 4x2.5/2-Gigabit ports • 2x10/1-Gigabit ports The following SFPs are supported: • GLC-BX-D • GLC-BX-U • GLC-SX-MMD • GLC-ZX-SMD • GLC-TE • SFP-10G-LR • SFP-10G-LR-S • SFP-10G-LRM • SFP-10G-LR-X • SFP-10G-SR • SFP-10G-SR-S • SFP-10G-SR-X • SFP-H10GB-CU1M • SFP-H10GB-CU1.5M [2] • SFP-H10GB-CU2M [2] • SFP-H10GB-CU2.5M [2] • SFP-H10GB-CU3M [2] • SFP-H10GB-CU5M [2] • SFP-H10GB-ACU7M • SFP-H10GB-ACU10M • FINISAR-LR – FTLX1471D3BCL [1] • FINISAR-SR – FTLX8574D3BCL [1]

[1] The FINISAR SFPs are not CISCO specific and some of the features like DOM may not work properly.
[2] Supported from Cisco IOS XE Bengaluru 17.6.3

Optics Modules

Cisco Catalyst 9800 Series Wireless Controller supports a wide range of optics. The list of supported optics is updated on a regular basis. See the tables at the following location for the latest transceiver module compatibility information:

https://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

Supported Hardware

The following table lists the supported virtual and hardware platforms. (See Table 13: Supported PIDs and Ports for the list of supported modules.)

Table 11: Supported Virtual and Hardware Platforms

Platform	Description
Cisco Catalyst 9800-80 Wireless Controller	A modular wireless controller with up to 100-GE modular uplinks and seamless software updates. The controller occupies a 2-rack unit space and supports multiple module uplinks.
Cisco Catalyst 9800-40 Wireless Controller	A fixed wireless controller with seamless software updates for mid-size to large enterprises. The controller occupies a 1-rack unit space and provides four 1-GE or 10-GE uplink ports.
Cisco Catalyst 9800-L Wireless Controller	The Cisco Catalyst 9800-L Wireless Controller is the first low-end controller that provides a significant boost in performance and features.
Cisco Catalyst 9800 Wireless Controller for Cloud	A virtual form factor of the Catalyst 9800 Wireless Controller that can be deployed in a private cloud (supports VMware ESXi, Kernel-based Virtual Machine [KVM], Microsoft Hyper-V, and Cisco Enterprise NFV Infrastructure Software [NFVIS] on Enterprise Network Compute System [ENCS] hypervisors), or in the public cloud as Infrastructure as a Service (IaaS) in Amazon Web Services (AWS), Google Cloud Platform (GCP) marketplace, and Microsoft Azure.
Cisco Catalyst 9800 Embedded Wireless Controller for Switch	The Catalyst 9800 Wireless Controller software for the Cisco Catalyst 9000 switches brings the wired and wireless infrastructure together with consistent policy and management. This deployment model supports only Software Defined-Access (SDA), which is a highly secure solution for small campuses and distributed branches.

The following table lists the host environments supported for private and public cloud.

Table 12: Supported Host Environments for Public and Private Cloud

Host Environment	Software Version
VMware ESXi	• VMware ESXi vSphere 6.0, 6.5, 6.7, and 7.0 • VMware ESXi vCenter 6.0, 6.5, 6.7, and 7.0

Host Environment	Software Version
KVM	• Linux KVM-based on Red Hat Enterprise Linux 7.6, 7.8, and 8.2 • Ubuntu 16.04.5 LTS, Ubuntu 18.04.5 LTS, Ubuntu 20.04.5 LTS
AWS	AWS EC2 platform
NFVIS	ENCS 3.8.1 and 3.9.1
GCP	GCP marketplace
Microsoft Hyper-V	Windows Server 2019, and Windows Server 2016 (Version 1607) with Hyper-V Manager (Version 10.0.14393)
Microsoft Azure	Microsoft Azure

The following table lists the supported Cisco Catalyst 9800 Series Wireless Controller hardware models.

The base PIDs are the model numbers of the controller.

The bundled PIDs indicate the orderable part numbers for the base PIDs that are bundled with a particular network module. Running the **show version**, **show module**, or **show inventory** command on such a controller (bundled PID) displays its base PID.

Note that unsupported SFPs will bring down a port. Only Cisco-supported SFPs (GLC-LH-SMD and GLC-SX-MMD) should be used on the route processor (RP) ports of C9800-80-K9 and C9800-40-K9.

Table 13: Supported PIDs and Ports

The following table lists the supported SFP models.

Optics Modules

The Cisco Catalyst 9800 Series Wireless Controller supports a wide range of optics. The list of supported optics is updated on a regular basis. See the tables at the following location for the latest transceiver module compatibility information:

https://www.cisco.com/c/en/us/support/interfaces-modules/transceiver-modules/products-device-support-tables-list.html

Supported APs

The following Cisco APs are supported in this release.

Indoor Access Points

- Cisco Catalyst 9105AX (I) Access Points
  - VID 04 or later - supported from 17.6.4
  - VID 03 or earlier - supported in all 17.6.x releases
- Cisco Catalyst 9105AX (W) Access Points

  - VID 02 or later - supported from 17.6.4
  - VID 01 or earlier - supported in all 17.6.x releases
- Cisco Catalyst 9115AX (I/E) Access Points
- Cisco Catalyst 9117AX (I) Access Points
- Cisco Catalyst 9120AX (I/E) Access Points
  - VID 07 or later - supported from 17.6.4
  - VID 06 or earlier - supported in all 17.6.x releases
- Cisco Catalyst 9120AX (P) Access Points
- Cisco Catalyst 9130AX (I/E) Access Points
  - VID 03 or later - supported from 17.6.4
  - VID 02 or earlier - supported in all 17.6.x releases

  (For information about Cisco Catalyst 9105, 9120, or 9130 Access Points version support, see the Field Notice 72424.)
- Cisco Aironet 1815 (I/W), 1830 (I), 1840 (I), and 1852 (I/E) Access Points
- Cisco Aironet 2800 (I/E) Series Access Points
- Cisco Aironet 3800 (I/E/P) Series Access Points
- Cisco Aironet 4800 Series Access Points

Outdoor Access Points

- Cisco Aironet 1540 Series Access Points
- Cisco Aironet 1560 Series Access Points
- Cisco Industrial Wireless 3700 Series Access Points
- Cisco Catalyst Industrial Wireless 6300 Heavy Duty Series Access Point
- Cisco 6300 Series Embedded Services Access Point
- Cisco Catalyst 9124AX (I/D/E) Access Points

Integrated Access Points

- Integrated Access Point on Cisco 1100 ISR (ISR-AP1100AC-x, ISR-AP1101AC-x, and ISR-AP1101AX-x)

Network Sensor

- Cisco Aironet 1800s Active Sensor

Supported Access Point Channels and Maximum Power Settings

Supported access point channels and maximum power settings on Cisco APs are compliant with the regulatory specifications of channels, maximum power levels, and antenna gains of every country in which the access points are sold. For more information about the supported access point transmission values in Cisco IOS XE software releases, see the *Detailed Channels and Maximum Power Settings* document at https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-17/products-technical-reference-list.html.

For information about Cisco Wireless software releases that support specific Cisco AP modules, see the "Software Release Support for Specific Access Point Modules" section in the *Cisco Wireless Solutions Software Compatibility Matrix* document.

Compatibility Matrix

The following table provides software compatibility information. For more information, see Cisco Wireless Solutions Software Compatibility Matrix

Table 14: Compatibility Information

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco Catalyst Center	Cisco CMX
Bengaluru 17.6.x	3.1 3.0 2.7 2.6 2.4	3.10 3.9	8.10.196.0 8.10.190.0 8.10.185.0 8.10.171.0 8.10.162.0 8.10.151.0 8.10.142.0 8.10.130.0 8.8.130.0 8.5.182.104 8.5.176.0 8.5.176.2 8.5.164.0 8.5.164.216	See Cisco Catalyst Center Compatibility Information	11.0 10.6.3

GUI System Requirements

The following subsections list the hardware and software required to access the Cisco Catalyst 9800 Controller GUI.

Table 15: Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[3]	512 MB[4]	256	1280 x 800 or higher	Small

[3] We recommend 1 GHz.
[4] We recommend 1-GB DRAM.

Software Requirements

Operating Systems:

- Windows 7 or later
- Mac OS X 10.11 or later

Browsers:

- Google Chrome: Version 59 or later (on Windows and Mac)
- Microsoft Edge: Version 40 or later (on Windows)
- Safari: Version 10 or later (on Mac)
- Mozilla Firefox: Version 60 or later (on Windows and Mac)

Note Firefox Version 63.x is not supported.

The controller GUI uses Virtual Terminal (VTY) lines for processing HTTP requests. At times, when multiple connections are open, the default number of VTY lines of 15 set by the device might get exhausted. Therefore, we recommend that you increase the number of VTY lines to 50.

To increase the VTY lines in a device, run the following commands in the following order:

1. **device#** configure terminal
2. **device(config)#** line vty 50

   A best practice is to configure the service tcp-keepalives to monitor the TCP connection to the device.
3. **device(config)#** service tcp-keepalives-in
4. **device(config)#** service tcp-keepalives-out

Before You Upgrade

Ensure that you familiarize yourself with the following points before proceeding with the upgrade:

- When you upgrade from Cisco IOS XE Dublin 17.12.3 to 17.12.4 or Cisco IOS XE 17.15.1, the Cisco Catalyst Wi-Fi 6 APs fail to upgrade the AP image.

  Workaround:

  - Reboot the impacted APs through the power cycle.

  For more information, see CSCwm08044

Warning APs that are upgraded to Release 17.6.x cannot join controllers that are running AireOS versions earlier than 8.10.162.0, 8.5MR8, or 8.5.176.2(IRCM).

Caution During controller upgrade or reboot, if route processor ports are connected to any Cisco switch, ensure that the route processor ports are not flapped (shut/no shut process). Otherwise, it may lead to a kernel crash.

- ISSU feature is supported only within and between major releases, for example, 17.3.x (within a release) and 17.3.x to 17.6.x (among major releases).
- Controller upgrade from Cisco IOS XE Bengaluru 17.3.x to Cisco IOS XE Bengaluru 17.6.x or Cisco IOS XE Cupertino 17.9.x or later using ISSU may fail if the **domain** command is configured. Ensure that you run the **no domain** command before starting an ISSU upgrade because the **domain** command has been removed from Cisco IOS XE Bengaluru 17.6.x.
- Controller upgrade from Cisco IOS XE Bengaluru 17.3.x to any release using ISSU may fail if the **snmp-server enable traps hsrp** command is configured. Ensure that you remove the **snmp-server enable traps hsrp** command from the configuration before starting an ISSU upgrade because the **snmp-server enable traps hsrp** command has been removed from Cisco IOS XE Bengaluru 17.4.x.
- Controller upgrade to Cisco IOS XE Dublin 17.12.x from any prior release using ISSU may fail if the **snmp-server enable traps license** command is configured. Ensure that you remove the **snmp-server enable traps license** command from the configuration before starting an ISSU upgrade because the **snmp-server enable traps license** command has been removed from Cisco IOS XE Dublin 17.12.x.
- Rolling AP upgrade, which is a part of the ISSU feature, is not supported for mesh APs.
- Ensure that you add Authentication and Key Management (AKM) setting when you configure WPA3. In older releases, this scenario was not mandatory which resulted in an invalid configuration. However, from 17.9 and higher releases, this invalid scenario is detected and prevented.

Cisco Wave 2 APs may get into a boot loop when upgrading software over a WAN link. For more information, see: https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/220443-how-to-avoid-boot-loop-due-to-corrupted.html.

The following Wave 1 APs are not supported from 17.4 to 17.9.2, 17.10.x, 17.11.x, 17.13.x, 17.14.x, and 17.15.x:

- **Cisco Aironet 1570 Series Access Point**
- **Cisco Aironet 1700 Series Access Point**
- **Cisco Aironet 2700 Series Access Point**
- **Cisco Aironet 3700 Series Access Point**

Note

- Support for the above APs was reintroduced from Cisco IOS XE Cupertino 17.9.3.
- Support for these APs does not extend beyond the normal product lifecycle support. Refer to the individual End-of-Support bulletins on Cisco.com.
- Feature support is on parity with the 17.3.x release. Features introduced in 17.4.1 or later are not supported on these APs in the 17.9.3 release.
- You can migrate directly to 17.9.3 from 17.3.x, where x=4c or later.

- From Cisco IOS XE Dublin 17.10.x, Key Exchange and MAC algorithms like diffie-hellman-group14-sha1, hmac-sha1, hmac-sha2-256, and hmac-sha2-512 are not supported by default and it may impact some SSH clients that only support these algorithms. If required, you can add them manually. For information on manually adding these algorithms, see the **SSH Algorithms for Common Criteria Certification** document available at: https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m_sec-secure-shell-algorithm-ccc.html
- If APs fail to detect the backup image after running the **archive download-sw** command, perform the following steps:

  1. Upload the image using the **no-reload** option of the **archive download-sw** command:

     ```
     Device# archive download-sw /no-reload tftp://<tftp_server_ip>/<image_name>
     ```

  2. Restart the CAPWAP process using **capwap ap restart** command. This allows the AP to use the correct backup image after the restart (reload is not required.)

     ```
     Device# capwap ap restart
     ```

Caution The AP will lose connection to the controller during the join process. When the AP joins the new controller, it will see a new image in the backup partition. So, the AP will not download a new image from the controller.

- You might observe a high Confd CPU when full synchronization occurs between NETCONF datastore and Cisco IOS configuration. This behavior is normal and is triggered by the **line vty** command.
- The controller reloads automatically when a cold patch is applied using web UI. This behavior is applicable to 17.3.x and 17.6.x releases.
- From Cisco IOS XE Amsterdam 17.3.1 onwards, the Cisco Catalyst 9800-CL Wireless Controller requires 16 GB of disk space for new deployments.

If you are upgrading to Cisco IOS XE Amsterdam 17.3.x from a previous release, resizing of disk space is not supported. If the current disk space is lesser than 16 GB, you need to redeploy the VM to meet the new disk space requirements.

- Fragmentation lower than 1500 is not supported for the RADIUS packets generated by wireless clients in the Gi0 (OOB) interface.
- When you upgrade from Cisco IOS XE Bengaluru 17.4.1 to Cisco IOS XE Bengaluru 17.6.x, the controller does not send all telemetry information using gather points or Xpaths.
- Cisco IOS XE allows you to encrypt all the passwords used on the device. This includes user passwords and SSID passwords (PSK). For more information, see the "Password Encryption" section of the Cisco Catalyst 9800 Series Configuration Best Practices document.
- While upgrading to Cisco IOS XE 17.3.x and later releases, if the **ip http active-session-modules none** command is enabled, you will not be able to access the controller GUI using HTTPS. To access the GUI using HTTPS, run the following commands in the order specified below:

  1. **ip http session-module-list pkilist OPENRESTY_PKI**
  2. **ip http active-session-modules pkilist**

- Cisco Aironet 1815T OfficeExtend Access Point will be in local mode when connected to the controller. However, when it functions as a standalone AP, it gets converted to FlexConnect mode.
- The Cisco Catalyst 9800-L Wireless Controller may fail to respond to the BREAK signals received on its console port during boot time, preventing users from getting to the ROMMON. This problem is observed on the controllers manufactured until November 2019, with the default config-register setting of 0x2102. This problem can be avoided if you set config-register to 0x2002. This problem is fixed in the 16.12(3r) ROMMON for Cisco Catalyst 9800-L Wireless Controller. For information about how to upgrade the ROMMON, see the Upgrading ROMMON for Cisco Catalyst 9800-L Wireless Controllers section of the Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers document.
- By default, the controller uses a TFTP block size value of 512, which is the lowest possible value. This default setting is used to ensure interoperability with legacy TFTP servers. If required, you can change the block size value to 8192 to speed up the transfer process, using the **ip tftp blocksize** command in global configuration mode.
- We recommend that you configure the **password encryption aes** and the **key config-key password-encrypt** *key* commands to encrypt your password.
- If the following error message is displayed after a reboot or system crash, we recommend that you regenerate the trustpoint certificate:

  ```
  ERR_SSL_VERSION_OR_CIPHER_MISMATCH
  ```

  Use the following commands in the order specified below to generate a new self-signed trustpoint certificate:

  1. device# **configure terminal**
  2. device(config)# **no crypto pki trustpoint** *trustpoint_name*
  3. device(config)# **no ip http server**
  4. device(config)# **no ip http secure-server**

5. device(config)# **ip http server**
6. device(config)# **ip http secure-server**
7. device(config)# **ip http authentication** *local/aaa*

- Do not deploy OVA files directly to VMware ESXi 6.5. We recommend that you use an OVF tool to deploy the OVA files.
- Ensure that you remove the controller from Cisco Prime Infrastructure before disabling or enabling Netconf-YANG. Otherwise, the system may reload unexpectedly.
- Unidirectional Link Detection (UDLD) protocol is not supported.
- SIP media session snooping is not supported on FlexConnect local switching deployments.
- The Cisco Catalyst 9800 Series Wireless Controllers (C9800-CL, C9800-L, C9800-40, and C9800-80) support a maximum of 14,000 leases with internal DHCP scope.
- Configuring the mobility MAC address using the **wireless mobility mac-address** command is mandatory for both HA and 802.11r.
- If you have Cisco Catalyst 9120 (E/I/P) and Cisco Catalyst 9130 (E) APs in your network and you want to downgrade, use only Cisco IOS XE Gibraltar 16.12.1t. Do not downgrade to Cisco IOS XE Gibraltar 16.12.1s.
- The following SNMP variables are not supported:
  - CISCO-LWAPP-WLAN-MIB: cLWlanMdnsMode
  - CISCO-LWAPP-AP-MIB.my: cLApDot11IfRptncPresent, cLApDot11IfDartPresent
- If you are upgrading from Cisco IOS XE Gibraltar 16.11.x or an earlier release, ensure that you unconfigure the *advipservices* boot-level licenses on both the active and standby controllers using the **no license boot level advipservices** command before the upgrade. Note that the **license boot level advipservices** command is not available in Cisco IOS XE Gibraltar 16.12.1s and 16.12.2s.
- The Cisco Catalyst 9800 Series Wireless Controller has a service port that is referred to as *GigabitEthernet 0* port.

  The following protocols and features are supported through this port:
  - Cisco Catalyst Center
  - Cisco Smart Software Manager
  - Cisco Prime Infrastructure
  - Telnet
  - Controller GUI
  - DNS
  - File transfer
  - GNMI
  - HTTP

- HTTPS
- LDAP
- Licensing for Smart Licensing feature to communicate with CSSM
- Netconf
- NetFlow
- NTP
- RADIUS (including CoA)
- Restconf
- SNMP
- SSH
- SYSLOG
- TACACS+

- During device upgrade using GUI, if a switchover occurs, the session expires and the upgrade process gets terminated. As a result, the GUI cannot display the upgrade state or status.
- From Cisco IOS XE Bengaluru 17.4.1 onwards, the telemetry solution provides a name for the receiver address instead of the IP address for telemetry data. This is an additional option. During the controller downgrade and subsequent upgrade, there is likely to be an issue—the upgrade version uses the newly named receivers, and these are not recognized in the downgrade. The new configuration gets rejected and fails in the subsequent upgrade. Configuration loss can be avoided when the upgrade or downgrade is performed from Cisco Catalyst Center.
- From Cisco IOS XE Bengaluru 17.4.1 onwards, session timeout under the policy profile is supported.
- Twinax's Small Form-factor Pluggable (SFP) modules are supported only on built-in (fixed) data ports of the Cisco Catalyst 9800-80 Wireless Controller and the Cisco Catalyst 9800-40 Wireless Controller. The Cisco Catalyst 9800-80 Wireless Controller does not support Twinax SFPs in the Ethernet port adapter (EPA) slot or any other port.
- Communication between Cisco Catalyst 9800 Series Wireless Controller and Cisco Prime Infrastructure uses different ports:
  - All the configurations and templates available in Cisco Prime Infrastructure are pushed through SNMP and CLI, using UDP port 161.
  - Operational data for controller is obtained over SNMP, using UDP port 162.
  - AP and client operational data leverage streaming telemetry:
    - Cisco Prime Infrastructure to controller: TCP port 830 is used by Cisco Prime Infrastructure to push the telemetry configuration to the controller (using NETCONF).
    - Controller to Cisco Prime Infrastructure: TCP port 20828 is used for Cisco IOS XE 16.10.x and 16.11.x, and TCP port 20830 is used for Cisco IOS XE 16.12.x, 17.1.x and later releases.

- To migrate public IP address from 16.12.x to 17.x. ensure that you configure the **service internal** command. If you do not configure the **service internal** command, the IP address does not get carried forward.
- RLAN support with Virtual Routing and Forwarding (VRF) is not available.
- When you encounter the SNMP error *SNMP_ERRORSTATUS_NOACCESS 6*, it means that the specified SNMP variable is not accessible.
- We recommend that you perform a controller reload whenever there is a change in the controller's clock time to reflect an earlier time.

Note The DTLS version (DTLSv1.0) is deprecated for Cisco Aironet 1800 based on latest security policies. Therefore, any new out-of-box deployments of Cisco Aironet 1800 APs will fail to join the controller and you will get the following error message:

```
%APMGR_TRACE_MESSAGE-3-WLC_GEN_ERR: Chassis 1 R0/2: wncd: Error in AP Join, AP <AP-name>,
mac:<MAC-address>Model AIR-AP1815W-D-K9, AP negotiated unexpected DTLS version v1.0
```

To onboard new Cisco Aironet 1800 APs and to establish a CAPWAP connection, explicitly set the DTLS version to 1.0 in the controller using the following configuration:

```
config terminal
ap dtls-version dtls_1_0
end
```

Note that setting the DTLS version to 1.0 affects all the existing AP CAPWAP connections. We recommend that you apply the configuration only during a maintenance window. After the APs download the new image and join the controller, ensure that you remove the configuration.

To upgrade the field programmable hardware devices for Cisco Catalyst 9800 Series Wireless Controllers, see *Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers*.

Important Before you begin a downgrade process, you must manually remove the configurations which are applicable in the current version but not in older version. Otherwise, you might encounter an unexpected behavior.

- When you downgrade an AP from a higher version to Cisco IOS XE Amsterdam 17.3.x, the AP will not be accessible through SSH or the console due to the denial of the **enable** password, when the AP has not yet joined a controller. If the AP joins a controller, then the AP becomes accessible without any password denial.

Upgrade Path to Cisco IOS XE Bengaluru 17.6.x

Table 16: Upgrade Path to Cisco IOS XE Bengaluru 17.6.x Release

Current Software	Upgrade Path to Cisco IOS XE Bengaluru 17.6.x Release
16.10.x	Upgrade first to 16.12.5 and then to 17.6.x.

Current Software	Upgrade Path to Cisco IOS XE Bengaluru 17.6.x Release
16.11.x	Upgrade first to 16.12.5 and then to 17.6.x.
16.12.x	You can upgrade directly to 17.6.x.
17.1.x	Upgrade first to 17.3 and then to 17.6.x.
17.2.x	Upgrade first to 17.3 and then to 17.6.x.
17.3.x	You can upgrade directly to 17.6.x.
17.4.x	You can upgrade directly to 17.6.x.
17.5.x	You can upgrade directly to 17.6.x.

Upgrading the Controller Software

This section describes the various aspects of upgrading the controller software.

For information on the upgrade process and the methods to upgrade the Cisco Catalyst 9800 Series Wireless Controller software, see the "Upgrading the Cisco Catalyst 9800 Wireless Controller Software" chapter of the *Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide*.

The Cisco Catalyst 9800 Wireless Controller may crash during wncmrgd process if downgraded from 17.9.2 to 17.6.4. To avoid this, we recommend that you downgrade to Cisco IOS XE Bengaluru 17.6.4 from Cisco IOS XE Cupertino 17.9.x after removing the controller from Cisco DNAC inventory.

Finding the Software Version

The package files for the Cisco IOS XE software are stored in the system board flash device (flash:).

Use the **show version** privileged EXEC command to see the software version that is running on your controller.

Note Although the **show version** output always shows the software image running on the controller, the model name shown at the end of the output is the factory configuration, and does not change if you upgrade the software license.

Use the **show install summary** privileged EXEC command to see the information about the active package.

Use the **dir** *filesystem:* privileged EXEC command to see the directory names of other software images that you have stored in flash memory.

Software Images

- **Release**: Cisco IOS XE Bengaluru 17.6.x
- **Image Names (9800-80, 9800-40, and 9800-L)**:
  - C9800-80-universalk9_wlc.17.06.x.SPA.bin

- C9800-40-universalk9_wlc.17.06.x.SPA.bin
- C9800-L-universalk9_wlc.17.06.x.SPA.bin

- **Image Names (9800-CL)**:
  - **Cloud**: C9800-CL-universalk9.17.06.x.SPA.bin
  - **Hyper-V/ESXi/KVM**: C9800-CL-universalk9.17.06.x.iso, C9800-CL-universalk9.17.06.x.ova
  - **KVM**: C9800-CL-universalk9.17.06.x.qcow2
  - **NFVIS**: C9800-CL-universalk9.17.06.x.tar.gz

Software Installation Commands

Cisco IOS XE, Bengaluru, 17.6.x	
To install and activate a specified file, and to commit changes to be persistent across reloads, run the following command: **device# install add file** *filename* **[activate |commit]** To separately install, activate, commit, end, or remove the installation file, run the following command: **device# install ?** **Note** We recommend that you use the GUI for installation.	
add file tftp: *filename*	Copies the install file package from a remote location to a device, and performs a compatibility check for the platform and image versions.
activateauto-abort-timer]	Activates the file and reloads the device. The **auto-abort-timer** keyword automatically rolls back image activation.
commit	Makes changes that are persistent over reloads.
rollback to committed	Rolls back the update to the last committed version.
abort	Cancels file activation, and rolls back to the version that was running before the current installation procedure started.
remove	Deletes all unused and inactive software installation files.

Licensing

The Smart Licensing Using Policy feature is automatically enabled on the controller. This is also the case when you upgrade to this release. By default, your Smart Account and Virtual Account in Cisco Smart Software Manager (CSSM) are enabled for Smart Licensing Using Policy. For more information, see Smart Licensing Using Policy.

For a more detailed overview on Cisco Licensing, see cisco.com/go/licensingguide.

Interoperability with Clients

This section describes the interoperability of the controller software with client devices.

The following table lists the configurations used for testing client devices.

Table 17: Test Configuration for Interoperability

Hardware or Software Parameter	Hardware or Software Type
Release	Cisco IOS XE, Bengaluru, 17.6.x
Cisco Wireless Controller	See Supported Hardware, on page 23.
Access Points	See Supported APs.
Radio	• 802.11ax • 802.11ac • 802.11a • 802.11g • 802.11n
Security	Open, PSK (WPA2-AES), 802.1X (WPA2-AES) (EAP-FAST, EAP-TLS) 802.11ax
RADIUS	See Compatibility Matrix, on page 26.
Types of tests	Connectivity, traffic (ICMP), and roaming between two APs

The following table lists the client types on which the tests were conducted. Client types included laptops, hand-held devices, phones, and printers.

Table 18: Client Types

Client Type and Name	Driver or Software Version
Wi-Fi 6 Devices (Mobile Phone and Laptop)	
Apple iPhone 11	iOS 14.1
Apple iPhone SE 2020	iOS 14.1
Dell Intel AX1650w	Windows 10 (21.90.2.1)
Dell Latitude 5491 (Intel AX200)	Windows 10 Pro (21.40.2)
Samsung S20	Android 10
Samsung S10 (SM-G973U1)	Android 9.0 (One UI 1.1)
Samsung S10e (SM-G970U1)	Android 9.0 (One UI 1.1)

Client Type and Name	Driver or Software Version
Samsung Galaxy S10+	Android 9.0
Samsung Galaxy Fold 2	Android 10
Samsung Galaxy Flip Z	Android 10
Samsung Note 20	Android 10
Laptops	
Acer Aspire E 15 E5-573-3870 (Qualcomm Atheros QCA9377)	Windows 10 Pro (12.0.0.832)
Apple Macbook Air 11 inch	OS Sierra 10.12.6
Apple Macbook Air 13 inch	OS Catalina 10.15.4
Apple Macbook Air 13 inch	OS High Sierra 10.13.4
Macbook Pro Retina	OS Mojave 10.14.3
Macbook Pro Retina 13 inch early 2015	OS Mojave 10.14.3
Dell Inspiron 2020 Chromebook	Chrome OS 75.0.3770.129
Google Pixelbook Go	Chrome OS 84.0.4147.136
HP chromebook 11a	Chrome OS 76.0.3809.136
Samsung Chromebook 4+	Chrome OS 77.0.3865.105
Dell Latitude 3480 (Qualcomm DELL wireless 1820)	Win 10 Pro (12.0.0.242)
Dell Inspiron 15-7569 (Intel Dual Band Wireless-AC 3165)	Windows 10 Home (18.32.0.5)
Dell Latitude E5540 (Intel Dual Band Wireless AC7260)	Windows 7 Professional (21.10.1)
Dell XPS 12 v9250 (Intel Dual Band Wireless AC 8260)	Windows 10 (19.50.1.6)
Dell Latitude 5491 (Intel AX200)	Windows 10 Pro (21.40.2)
Dell XPS Latitude12 9250 (Intel Dual Band Wireless AC 8260)	Windows 10 Home (21.40.0)
Lenovo Yoga C630 Snapdragon 850 (Qualcomm AC 2x2 Svc)	Windows 10 (1.0.10440.0)
Lenovo Thinkpad Yoga 460 (Intel Dual Band Wireless-AC 9260)	Windows 10 Pro (21.40.0)
Note For clients using Intel wireless cards, we recommend that you to update to the latest Intel wireless drivers if the advertised SSIDs are not visible.	
Tablets	

Client Type and Name	Driver or Software Version
Apple iPad Pro	iOS 13.5
Apple iPad Air2 MGLW2LL/A	iOS 12.4.1
Apple iPad Mini 4 9.0.1 MK872LL/A	iOS 11.4.1
Apple iPad Mini 2 ME279LL/A	iOS 12.0
Microsoft Surface Pro 3 – 11ac	Qualcomm Atheros QCA61x4A
Microsoft Surface Pro 3 – 11ax	Intel AX201 chipset. Driver v21.40.1.3
Microsoft Surface Pro 7 – 11ax	Intel Wi-Fi chip (HarrisonPeak AX201) (11ax, WPA3)
Microsoft Surface Pro X – 11ac & WPA3	WCN3998 Wi-Fi Chip (11ac, WPA3)
Mobile Phones	
Apple iPhone 5	iOS 12.4.1
Apple iPhone 6s	iOS 13.5
Apple iPhone 8	iOS 13.5
Apple iPhone X MQA52LL/A	iOS 13.5
Apple iPhone 11	iOS 14.1
Apple iPhone SE MLY12LL/A	iOS 11.3
ASCOM SH1 Myco2	Build 2.1
ASCOM SH1 Myco2	Build 4.5
ASCOM Myco 3 v1.2.3	Android 8.1
Drager Delta	VG9.0.2
Drager M300.3	VG2.4
Drager M300.4	VG2.4
Drager M540	DG6.0.2 (1.2.6)
Google Pixel 2	Android 10
Google Pixel 3	Android 11
Google Pixel 3a	Android 11
Google Pixel 4	Android 11
Huawei Mate 20 pro	Android 9.0
Huawei P20 Pro	Android 9.0
Huawei P40	Android 10
LG v40 ThinQ	Android 9.0
One Plus 8	Android 10

Client Type and Name	Driver or Software Version
Oppo Find X2	Android 10
Redmi K20 Pro	Android 10
Samsung Galaxy S7	Andriod 6.0.1
Samsung Galaxy S7 SM - G930F	Android 8.0
Samsung Galaxy S8	Android 8.0
Samsung Galaxy S9+ - G965U1	Android 9.0
Samsung Galaxy SM - G950U	Android 7.0
Sony Experia 1 ii	Android 10
Sony Experia xz3	Android 9.0
Xiaomi Mi10	Android 10
Spectralink 8744	Android 5.1.1
Spectralink Versity Phones 9540	Android 8.1
Vocera Badges B3000n	4.3.2.5
Vocera Smart Badges V5000	5.0.4.30
Zebra MC40	Android 5.0
Zebra MC40N0	Android 4.1.1
Zebra MC92N0	Android 4.4.4
Zebra TC51	Android 7.1.2
Zebra TC52	Android 8.1.0
Zebra TC55	Android 8.1.0
Zebra TC57	Android 8.1.0
Zebra TC70	Android 6.1
Zebra TC75	Android 6.1.1
Printers	
Zebra QLn320 Printer	LINK OS 6.3
Zebra ZT230 Printer	LINK OS 6.3
Zebra ZQ310 Printer	LINK OS 6.3
Zebra ZD410 Printer	LINK OS 6.3
Zebra ZT410 Printer	LINK OS 6.3
Zebra ZQ610 Printer	LINK OS 6.3
Zebra ZQ620 Printer	LINK OS 6.3

Client Type and Name	Driver or Software Version
Wireless Module	
Intel 11ax 200	Driver v22.20.0
Intel AC 9260	Driver v21.40.0
Intel Dual Band Wireless AC 8260	Driver v19.50.1.6

Issues

Issues describe unexpected behavior in Cisco IOS releases in a product. Issues that are listed as Open in a prior release are carried forward to the next release as either Open or Resolved.

Note All incremental releases contain fixes from the current release.

Cisco Bug Search Tool

The Cisco Bug Search Tool (BST) allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The BST is designed to improve the effectiveness in network risk management and device troubleshooting. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of an issue, click the corresponding identifier.

Open Caveats for Cisco IOS XE Bengaluru 17.6.8

Caveat ID	Description
CSCwj92716	Native mode and IOx application both use the IoT UART interface resulting in continuous IoT chip resets
CSCwi28174	Multicast L3 packets are sent in native VLAN when VLAN ID 1 is selected in policy profile with AAA override

Open Caveats for Cisco IOS XE, Bengaluru, 17.6.7

Identifier	Headline
CSCwi64652	Cisco Catalyst 9105AX APs do not reset Bluetooth Low Energy (BLE) interface after 100 attempts.
CSCwi19804	Cisco Catalyst 9105, 9115, or 9120 Series APs: Radio is misconfigured after AP reloads when admin state down.
CSCwi81972	Cisco COS AP checks DELETE_VAP_PAYLOAD CAPWAP payload sanity before blindly deleting.

Identifier	Headline
CSCwi06785	Controller does not send IPv4 GARPs or IPv6 NA for wireless client in RUN state after a switchover.
CSCwh80060	Cisco COS APs connected to the controller loses WLAN VLAN mapping intermittently in FlexConnect mode.
CSCwh57076	Controller does not forward the broadcast Address Resolution Protocol (ARP) request to the wireless client.
CSCwh02986	Cisco Catalyst 9120 AP transmit power in dbm does not match between controller or AP.
CSCwi75759	Cisco Catalyst 9800-40 Wireless Controller reloads due to Critical process WNCd fault in rp_0_1 (rc=139).
CSCwi83124	Controller GUI pop-ups are not displayed correctly in Dark mode.
CSCwf61881	Cisco Catalyst 9166D1 AP changes from US to UX country domain when AP moves from LPi mode to Standard Power (SP) mode.
CSCwi64010	Controller accepts the reserved IPv6 multicast address to be configured as Mobility multicast IPv6 address.
CSCwi47294	The per client rate limit does not work when using FlexConnect local switching APs.
CSCwi48980	The local password policy in the controller does not take effect during Controller GUI login.
CSCwf83515	Inconsistent transmission power levels advertised in Country information of beacon frame causes client-side issues.
CSCwi03442	Cisco Catalyst 9130 AP does not honor the U-APSD trigger frame causing real-time protocol (RTP) stream disruption.

Open Caveats for Cisco IOS XE Bengaluru 17.6.6a

Identifier	Headline
CSCwc99359	The rogue rule configuration for delete classification does not take effect.
CSCwe28717	Certificate failure issues observed when joining APs to the controller using CMCA III certificate structure.
CSCwf22788	The **show wireless client summary detail** command does not show all IPv6 addresses.
CSCwh03842	Cisco Aironet 4800 Series AP beacons are missed intermittently on multiple BSSIDs.
CSCwh27366	Cisco Aironet 3800 Series AP experiences radio firmware crash.
CSCwf84639	Cisco Catalyst 9120 Series AP: XOR mode is not updated on the database.
CSCwe68984	Cisco Catalyst 9105 Series AP WGB does not send PMKID during reassociation.

Identifier	Headline
CSCwe11213	Cisco Catalyst 9130 Series AP crash observed due to radio failure.
CSCwf90946	Cisco Catalyst 9130 Series AP does not forward 802.1x identity request with wireless phones.
CSCwf73002	Unable to remove port security configurations under interface through NETCONF.
CSCwf53520	Kernel panic crash observed on Cisco Aironet 1815 Series AP.
CSCwf91445	The controller pushes accounting information for PSK local authentication WLANs.
CSCwd76693	Profile mismatch counter does not increase.
CSCwd79178	Cisco Aironet 1840 Series AP: OfficeExtend Access Point (OEAP) crashes due to radio recovery failure.
CSCwf93992	Cisco Aironet 2800 Series AP do not process EAP-TLS fragmented packets if there is a delay of more than 50 milliseconds.

Open Caveats for Cisco IOS XE, Bengaluru, 17.6.6

Identifier	Headline
CSCwc99359	The rogue rule configuration for delete classification does not take effect.
CSCwe28717	Certificate failure issues observed when joining APs to the controller using CMCA III certificate structure.
CSCwf22788	The **show wireless client summary detail** command does not show all IPv6 addresses.
CSCwh03842	Cisco Aironet 4800 Series AP beacons are missed intermittently on multiple BSSIDs.
CSCwh27366	Cisco Aironet 3800 Series AP experiences radio firmware crash.
CSCwf84639	Cisco Catalyst 9120 Series AP: XOR mode is not updated on the database.
CSCwe68984	Cisco Catalyst 9105 Series AP WGB does not send PMKID during reassociation.
CSCwe11213	Cisco Catalyst 9130 Series AP crash observed due to radio failure.
CSCwf90946	Cisco Catalyst 9130 Series AP does not forward 802.1x identity request with wireless phones.
CSCwf73002	Unable to remove port security configurations under interface through NETCONF.
CSCwf53520	Kernel panic crash observed on Cisco Aironet 1815 Series AP.
CSCwf91445	The controller pushes accounting information for PSK local authentication WLANs.
CSCwd76693	Profile mismatch counter does not increase.
CSCwd79178	Cisco Aironet 1840 Series AP: OfficeExtend Access Point (OEAP) crashes due to radio recovery failure.

Identifier	Headline
CSCwf93992	Cisco Aironet 2800 Series AP do not process EAP-TLS fragmented packets if there is a delay of more than 50 milliseconds.

Open Caveats for Cisco IOS XE, Bengaluru, 17.6.5

Caveat ID	Description
CSCwc32182	Cisco Aironet 1852 Access Point experiences radio firmware crash.
CSCwc75732	Cisco Aironet 4800 Access Point experiences radio firmware crash.
CSCwd10172	Cisco Catalyst 9115AXI Access Point deteccts invalid cookie and resets to ux domain.
CSCwd26693	The N+1 High Availability setup for FlexConnect APs are not working.
CSCwd46815	EAP-TLS is failing for the wired clients behind Mesh Access Points (MAP) in 2800/3800/4800/1562/6300 series APs.
CSCwd52745	Cisco Aironet 3802 Access Point experiences kernel crash.
CSCwd60034	Cisco Aironet 3800 Access Point experiences radio crash due to stuck beacon.
CSCwd79502	Controller is tracking stale entries due to which anchored client is getting IPv4 and IPv6 addresses at different VLANs.
CSCwd81523	Cisco Catalyst 9130 Access Point is not sending EAP_ID_RESP next assoc-req after Protected Management Frames (PMF) client tx deauth in middle of Extensible Authentication Protocol (EAP) handshake.
CSCwa14922	ICAP: Anomaly capture events for a client on Cisco Catalyst 9130 Access Point is often missing Packet Capture (PCAP).
CSCwb72924	FlexConnect client is intermittently unable to reconnect to an AP.
CSCwc10621	CleanAir statistics are not visible in Cisco Catalyst 9130 Access Points when joined to EWC.
CSCwc49970	Channel 165 is not allowed on Cisco Aironet 2800, 3800, 4800 Access Points.
CSCwd36552	Cisco Catalyst 9120 Access Point experiences vernel panic crash.
CSCwd41463	Cisco Aironet 3800 and 4800 Access Points stop sending Internet Group Management Protocol (IGMP) membership report.
CSCwd49166	Cisco Aironet 3800 Access Point is consistently reporting high QoS Basic Set Service (QBSS) load.

Caveat ID	Description
CSCwd83840	Wireless clients unable to connect to Cisco Aironet 1830 Access Point.
CSCwd08068	Cisco Aironet 1815W Access Point is crashing due to Out of Memory (OOM).
CSCwc99359	Rogue rule delete classification configuration is not working.
CSCwc74020	Allow wireless client IPv6 traffic coming with new src addresses without learning after 8 addresses.
CSCwd76693	Profile mismatch counter is not increasing.

Open Caveats for Cisco IOS XE, Bengaluru, 17.6.4

Caveat ID	Description
CSCwa12204	Controller does not send the right Association IDentifier (AID) causing APs to not accept new clients.
CSCwa31596	High channel utilization is observed when 9 or more clients use MS TEAMS in a Cisco Catalyst 9130 AP.
CSCwb71679	Cisco Aironet 4800 Series AP in 8.10.171.0 crash due to FIQ or NMI reset.
CSCwc02477	Cisco Catalyst 9130 AP does not transmit Extensible Authentication Protocol (EAP) identity request.
CSCvz30614	Cisco Aironet 1815m AP experiences high channel utilization in 5GHz radio with 40MHz.
CSCwa14922	Anomaly Capture events for a client in Cisco Catalyst 9130 AP is often missing Packet CAPture (PCAP).
CSCwb08291	Cisco Catalyst 9105AXW AP introduces latency when clients use RLAN ports.
CSCwc05350	CAPWAP MTU flapping occurs in COS APs due to asymmetric MTU between AP to controller and vice-versa.
CSCwc15898	Missing CleanAir data for 2.4GHz in Cisco Catalyst 9120 or 9130 series APs.
CSCwc55849	Cisco Catalyst 9800-80 Wireless Controller in High Availability experiences 100% CPU in all wncds after configuration change.
CSCwb47046	**wncmgrd** process memory leak is observed in Cisco IOS XE 17.8.
CSCwb77619	Four-way handshake is not completed in controller or Cisco Catalyst 9115 AP.

Caveat ID	Description
CSCwc05366	Wireless clients cannot reach each other as the ARP resolution fails when performing dynamic VLAN assignment using AAA.
CSCwc26105	High Availability split brain is observed in the controller due to multiple secondary address in the interface.
CSCwc40403	Users connecting to the dot1x SSID are disconnected with CO_CLIENT_DELETE_REASON_EXCLUDE_IP_THEFT delete code.
CSCwc42784	Client fails to connect when protocol based Quality of Service (QoS) is configured.
CSCwc51730	APs are unable to broadcast SSID after provisioning from Cisco DNAC.
CSCwc54370	Standby controller becomes the new active but does not send GARPs for Wireless Management Interface after joining High Availability pair again after network disconnection.
CSCwa93208	FlexConnect WLAN VLAN mapping disappears when using VLAN name defined in the Flex Profile.
CSCwb47040	Controller does not update RFID location properly.
CSCwb69343	6 GHz channels are displayed as 2.4 GHz when executing **show ap wlan summary** command.
CSCwb78191	AAA VLAN override is not considered during Identity PSK (iPSK) authentication and anchor WLAN.
CSCwc17774	Few OIDs in CISCO-ENHANCED-MEMPOOL-MIB display No instance after switchover in Cisco IOS XE 17.6.1.
CSCwc26819	Controller does not send Logical Link Control (LLC) or eXchange IDentifier (XID) spoofed frames after a mobility event.
CSCwc28408	Crash happens intermittently in the controller when WNCd critical process failed.
CSCwc32746	Site tags are not load balanced correctly for each WNCd process.
CSCwc36125	Radio Resource Management (RRM) startup mode is triggered in every reboot as the controller does not keep track of the last state.
CSCwc41903	The LISP RELIABLE REGISTRATION related Syslog needs to be enhanced.
CSCwc24994	Cisco Aironet 3800 Series AP crashes due to kernel panic.
CSCwc30314	Cisco Aironet 4800 AP sends upstream DHCP packets in CAPWAP in FlexConnect local switching local DHCP policy.

Caveat ID	Description
CSCwc49992	Kernel panic - not syncing: Fatal exception "off_channel resp timeout".
CSCwc55632	Cisco Catalyst 9124 MAP fails to connect to Cisco Aironet 1562 RAP after the first reload of MAP.
CSCwc62749	Cisco Catalyst 9100 AP Plug and Play (PnP) is unable to resolve any public Network Time Protocol (NTP) server.
CSCwb79809	Upstream video traffic drops in Cisco Catalyst 9124 AP.
CSCwc38912	The Local Web Authentication (LWA) client gets deleted immediately when joining the Flex WLAN after a Site or Policy Tag update.
CSCwc49464	Cisco Catalyst 9115 and 9120 APs are stuck in boot loop due to signature verification failure.
CSCwc49970	Channel 165 is not allowed in Cisco Aironet 2800, 3800, or 4800 AP models.
CSCwc60964	Cisco Catalyst 9130 Series AP experiences kernel panic crash in NSS.
CSCwc62259	OEAP Cisco Aironet 1815T and 1810 with 802.1x supplicant configuration does not enter the FlexConnect Standalone state.
CSCwc64538	Cisco Catalyst 9100 AP does not transmit the directed broadcast over-the-air.

Open Caveats for Cisco IOS XE, Bengaluru, 17.6.3

Caveat ID	Description
CSCvx40586	Controller does not sort the RFID RSSI received from APs before sending 16 APs to the connector.
CSCwa99904	Cisco Catalyst 9800 Series Wireless Controller deletes client when it receives DHCP RELEASE during 802.1x and Posture Auth.
CSCvz39796	A large number of unwanted clean air or 11k related errors and messages are noticed at debug level adding to wncd CPU utilization.
CSCwa74884	Cisco Catalyst 9800 Series Wireless Controller sends wrong payload information to AP when mesh RRM is enabled or disabled.
CSCwa67566	Controller rejects clients with wrong PMKID when client moves from FT-AKM to dot1x-AKM.

Caveat ID	Description
CSCwa48644	The FortyGigabitEthernet 0/1/1 interfaces in Cisco Catalyst 9800-80 Wireless Controller is stuck in DOWN state after repeated HA failovers.
CSCwb24037	Client is unable to reassociate to the controller after failing the Broadcast Key rotation process.
CSCvy01360	Cisco Catalyst 9105, 9115, or 9120 Series APs report false radar detection.
CSCwa12204	Cisco Catalyst 9800 Series Wireless Controller does not send the right AID causing APs to not accept new clients.
CSCwa30802	MU sounding errors lead to TCQ stuck issue.
CSCwa31596	High channel utilization is observed when 9 or more clients use MS Teams in a Cisco Catalyst 9130 AP.
CSCwa42620	Cisco Catalyst 9130 APs drop traffic on air for Phoenix WinNonlin Application.
CSCwa49815	Controller running 8.10.151.0 experiences CleanAir sensor down.
CSCwa50159	Cisco Catalyst 9120 APs display high client count when neighboring APs have very few clients associated to it.
CSCwa54943	Cisco Aironet 1810 AP restarts abnormally on the controller due to Out of Memory.
CSCwa68709	Cisco Catalyst 9115 AP reports incorrect radar DFS channels in GUI.
CSCwa81190	Cisco Catalyst 9120 AP displays Null pointer de-reference when PC is at wlc_wnm_is_wnmsleeping.
CSCwa86610	Cisco Aironet 2802 and 3802 AP experiences kernel panic crash in 8.10.151.0.
CSCwa96198	Central Web Authentication (CWA) clients with Run state cannot go online even though they are in Run state.
CSCwa96429	Cisco Aironet 4800 APs cannot reach the default gateway after CTS manual configuration is added to the AP switchport.
CSCwa96749	Cisco Aironet 3800 series AP crashes due to kernel panic.
CSCwb19448	Cisco Catalyst 9117 AP crashes due to kernel panic in cisco_wlan_crypto_decap.
CSCwb68720	AP is sending ARP packet without VXLAN encapsulation.

Open Caveats for Cisco IOS XE, Bengaluru, 17.6.2

Caveat ID	Description
CSCvz30697	Cisco Catalyst 9120 AP and 8821 phone delays in downstream or signalling does not work.
CSCvz34172	Cisco Aironet 1832 AP experiences kernel panic while setting client ACL in Cisco IOS XE 17.3.4.
CSCvz38018	cEdge reloads unexpectedly when issuing OMP shutdown from the CLI.
CSCvz59068	Firmware crash observed in Cisco Catalyst 9117 Series APs.
CSCvz59191	APs do not send NDP packets on slot 1.
CSCvz60269	Sensord crash is observed in Cisco Catalyst 9130 AP after off_channel RX timeout.
CSCvz65712	Software crashes on process wcpd when C9130 AP is connected to the controller (17.6.1.13).
CSCvz77768	IOS AP brings the radio down after encountering DFS event even when non-DFS channels are available.
CSCvz91602	The Cisco Aironet 2800 APs with lower RSSI is populated in the neighbour list.
CSCvz93039	Cisco Catalyst 9120 AP crashes due to kernel panic after an upgrade from 17.3.3.26 to 17.3.4.30.
CSCvz95745	The CleanAir interference devices are not merged in clusters.
CSCvz65701	The controller does not respond to TCP, SSH, or RADIUS packets randomly.

Open Caveats for Cisco IOS XE, Bengaluru, 17.6.1

Caveat ID	Description
CSCvp88559	Cisco Aironet 1810W AP reloads unexpectedly due to kernel panic.
CSCvx67724	Cisco Aironet 1815 AP reloads unexpectedly due to out of memory.
CSCvx99197	Cisco Catalyst 9120 AP reloads unexpectedly after upgrading to 8.10.158.38.
CSCvy01360	Cisco Catalyst 9115 AP reports false radar detection on channels 100-112.
CSCvy03953	Cisco Catalyst 9130 AP reloads unexpectedly due to kernel panic.
CSCvy32730	Controller reloads unexpectedly on Pubd process in evlib.

Caveat ID	Description
CSCvy52874	Cisco Catalyst 9115 AP reloads unexpectedly after loading the 17.3.3 ES6 image.
CSCvy58888	Cisco Catalyst 9115 AP reloads unexpectedly on 17.3.3 ES7 image.
CSCvy69666	Cisco Aironet 3702 AP is generating AES-CCMP errors for PSK SSIDs.
CSCvy72869	AP data for \"total frame error over air\" & \"multicast/broadcast counter\" are missing.
CSCvy73836	Cisco Catalyst 9800-80 controller is going to ROMMON after multiple failovers due to power cycling.
CSCvy79320	Ping loss increases after two days of reboot.
CSCvy82669	Cisco AP is stuck in discovery process when switch side port VLAN is changed from quarantine to access.
CSCvy85178	Cisco Aironet 4800 APs in Enhanced Local Mode (ELM) and Local Mode on same controller/RF group are detecting each other as honeypot.
CSCvy87104	Cisco AP is not accepting clients in 2.4 GHz.
CSCvy88490	Cisco Aironet 2800 and 3800 APs reload unexpectedly and ends up with erased config and sshd service is unable to start.
CSCvy93675	uWGB client timeout value is not persistent after reload.
CSCvy92854	Cisco Catalyst 9130 AP running 17.5.1 fast-locate records are not sent even when client is connected to the AP.
CSCvy98805	Cisco Catalyst 9800-CL controller in standby mode is getting removed frequently after breaking HA.
CSCvz01677	Cisco Aironet 4800 Series AP reload unexpectedly on radio1 abnormally.
CSCvz06544	Controller reloads unexpectedly when enabling RMI+RP in WebUI before bringing HA connectivity up first.
CSCvs06271	RRM AP transmit power is not moving into the maximum or minimum configured power.
CSCvy15384	Datapath state mismatch strands wireless clients after roaming.
CSCvy30091	Cisco Catalyst 9120 AP stops transmitting frames to Macbook after session reauth.
CSCvy61073	Post-Auth access control lists (ACLs) are not working in the controller.

Caveat ID	Description
CSCvy76922	Memory leak is observed due to linux_iosd-imag.
CSCvy94725	Cisco Aironet 2800 and 3800 APs: Kernel panic driver crash is observed due to kernel panic on 2.4GHz radio.
CSCvy94730	Cisco Aironet 2800 and 3800 APs: Firmware crash is observed due to cmd timeout wifi0.
CSCvy95842	Cisco AP with non-EWC image is being factory reset due to DHCP 43 option with type f2 is set.
CSCvy96765	Cisco Catalyst 9120 AP fails to forward packets.
CSCvy97180	Cisco Catalyst 9130 APs display 100% channel utilization.
CSCvy98016	Cisco Aironet 2802 AP stops acknowledging frames till client sends BAR.
CSCvz02894	EAP-Request retry is not sent by the AP.
CSCvz03070	Cisco Aironet 1852 AP radio crash is observed.
CSCvz06937	Cisco Catalyst 9120 AP fimware crash is observed on radio 1.
CSCvv94885	The **show ap cdp neighbours** command displays switch name instead of domain name.
CSCvy76600	Flash memory cleanup is failing.
CSCvy91808	Intermediate-System to Intermediate-System (IS-IS) adjacency is not forming with point to point bridging.
CSCvy59897	Cisco Aironet 4800 AP is detecting its own BSSID as rogue.
CSCvz07708	CWA: Client prompted to web-auth login when roaming APs.

Resolved Caveats for Cisco IOS XE Bengaluru 17.6.8

Identifier	Headline
CSCwe81552	TPC does not work as expected when dual-band operates in 5-GHz or when Cisco Catalyst 9130 AP Slot 2 operates in client-serving role
CSCwi08147	Controller GUI does not allow modifying QoS policies without setting the “QoS SSID policy” in the policy profile
CSCwi81972	AP should perform a DELETE_VAP_PAYLOAD CAPWAP payload sanity check before blinding deleting
CSCwh09642	IP Theft is observed when the zone ID is 0x00000000

Identifier	Headline
CSCwh44793	Cisco Catalyst 9130 AP in Cisco IOS XE 17.3.6 fails to join back when fast transition data is set in BSSID after a site-tag change in the controller
CSCwh68219	Cisco Catalyst 91xx AP does not process the EAP-TLS Server Hello
CSCwb16423	The multicast DNS (mDNS) service policy update fails in SVI interfaces
CSCwh58099	Controller allows client reconnect after client deletion and Change of Authorization (CoA) termination
CSCwj26848	AP should perform a DELETE_VAP_PAYLOAD CAPWAP payload sanity check before blinding deleting
CSCwh33056	Policy tag description disappears after deleting WLAN location entries
CSCwh08892	Controller GUI displays only a blank page after the User Login page due to malformed user preference JSON
CSCwj66429	Cisco Catalyst 9115 AP ends abnormally with Kernel Panic as the reload reason
CSCwh49810	Audit session ID changes after inter-WNCD roam
CSCwj93906	Client authentication fails in Cisco Catalyst 9120 AP with "Sending Msg:2 in mode:2 to hostapd failed"

Resolved Caveats for Cisco IOS XE, Bengaluru, 17.6.7

Identifier	Headline
CSCwh68360	Cisco Catalyst 9120 AP experiences kernel panic due to wlc_key_set_data.
CSCwh59543	Radio firmware and Capwapd ends abnormally during scale longevitiy.
CSCwh50681	New SSID arp0v0 is broadcasted after a Cisco IOS XE Cupertino 17.9.3 wireless upgrade.
CSCwh09642	IP theft is observed when the zone ID is 0x00000000.
CSCwi92913	Cisco Catalyst 9105 and 9115 Series APs report false radar detection.
CSCwf13804	APs randomly fail to onboard new client associations with **netlink_socket_receive multicast_group 1 return failure: No buffer space available** errors.
CSCwh50813	The channel set fails when Cisco Aironet 1800 or 1500 APs try to come out after Dynamic Frequency Selection (DFS) NOL list.
CSCwi67013	Cisco Aironet 2800 AP in Taiwan domain does not send WiFi signals in channel 52, 120, 124, and 128.
CSCwh63270	Cisco Catalyst 9130AXI APs end abnormally due to radio failure.

Identifier	Headline
CSCwh27366	Cisco Aironet 3800 AP experiences firmware crash reset code 2 with crash signature gdp.
CSCwh81332	Cisco Catalyst 9130 APs experience kernel panic crash after an upgrade to Cisco IOS XE Bengaluru 17.6.6.
CSCwh20944	Cisco Catalyst 9120 AP ends abnormally due to kernel panic.
CSCwf13107	SCB Mismatch - radio ends abnormally during longevity test with Cisco Catalyst 9105 AP.
CSCwh33190	Cisco Catalyst 9115 AP (Local mode) ends abnormally due to kernel panic.
CSCwe11213	Cisco Catalyst 9130 AP ends abnormally due to radio recovery failure.
CSCwh68219	Cisco Catalyst 91xx AP does not process the EAP-TLS Server Hello.
CSCwh33056	Policy tag description disappears after deleting WLAN location entries.
CSCwi19481	Cisco Catalyst 9130 APs in Flex mode stops forwarding router advertisements after 4 to 6 hours of uptime.
CSCwh49810	Audit session ID changes after an inter-WNCD roam.
CSCwf53520	Cisco Aironet 1815 AP with Cisco IOS XE 17.9.2 experiences kernel panic.
CSCwe81552	Transmit Power Control (TPC) does not work as expected when secondary radio operates in 5-GHz band.
CSCwi91970	Transmission stuck issue is observed when Cisco Catalyst 9120 AP detects any radar event.
CSCwf91445	Controller pushes RADIUS accounting information to AP when SSID is configured for Local Auth with PSK as AKM.
CSCwe42200	Controller configured with RADIUS server using FQDN does not update properly during DNS periodic update.
CSCwh27425	Cisco Catalyst 9115AX AP does not forward a part of the CAPWAP data packets to the uplink direction.
CSCwb16423	The multicast DNS (mDNS) service policy updation fails under SVI interfaces.
CSCwh58099	Controller allows client reconnect after client deletion and Change of Authorization (CoA) termination.
CSCwh92425	Cisco Catalyst 9130 or 9136 APs do not respect the **Power Save** mode.
CSCwh54762	Cisco Catalyst 9120 AP ends abnormally due to **kernel panic - not syncing: assert:"0" failed: file "wlc_fifo.c:960"**.
CSCwh75431	Cisco Aironet 1830 or 1850 APs report false high channel utilization causing performance issues in 5-GHz band.

Identifier	Headline
CSCwi52692	Cisco Catalyst 9130 AP experiences issues when Cisco Universal Power over Ethernet (UPOE+) spare pair turn off CDP TLV message is triggered.
CSCwi08147	Controller GUI does not allow modifying QoS policies without QoS SSID policy being set.
CSCwh62342	AP FlexConnect as mDNS gateway does not respond correctly when LSS filter is enabled in 5-GHz band.
CSCwh74663	Cisco Aironet 2800, 3800, 4800, 1560, or 6300 APs do not send Quality of Service (QoS) data frames downstream.
CSCwi96089	APs do not plumb keys after a session timeout reauthentication.
CSCwh44793	Cisco Catalyst 9130 AP fails to join back until the old site-tag is applied after the site-tag is changed in Cisco IOS XE 17.3.6.
CSCwi22270	Cisco Catalyst 9120 AP experiences radio crash during longevity run with Cisco IOS XE 17.13.0.101 image.
CSCwi92439	Cisco Aironet 1815s AP reports high channel utilization in 5-GHz band.
CSCwi06055	Cisco Industrial Wireless 3702 AP radios are reset and stay down when board temperature is less than -20 degree Celsius.
CSCwi05672	Cisco Catalyst 9130 AP wireless driver does not decrypt the packet when IP packets are sourced from some wireless clients.
CSCwi28172	Cisco Catalyst 9120 AP experiences kernel panic when PC is at wlc_bmac_suspend_mac_and_wait+0x3c/0x488 [wl].
CSCwf44441	Cisco Catalyst 916(x) AP: Radio firmware ends abnormally with Thread ID: 0x00000069, Thread name: WLAN BE, PC : 0x4ae62d70(SF 06646968).
CSCwh61011	Cisco Catalyst 9120 and 9115 APs experience unexpected disjoins from the controller and does not establish DTLS again.

Resolved Caveats for Cisco IOS XE Bengaluru 17.6.6a

Identifier	Headline
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z.

Resolved Caveats for Cisco IOS XE, Bengaluru, 17.6.6

Identifier	Headline
CSCwd69780	Controller crashes and experiences CPU HOG in wncmgrd due to scale netflow.

Identifier	Headline
CSCwe38431	Controller moves SIP packets from CS3 to CS0 in upstream or downstream when voice Call Admission Control (CAC) is configured.
CSCwc32182	Cisco Aironet 1852 AP experiences radio firmware crash.
CSCvw70260	Cisco Aironet 1572EAC AP does not respond to the Canadian EIRP regulation.
CSCwf34100	Samsung device (Galaxy Tab S6 Lite - P610K) association is rejected with status code 40.
CSCwe07297	Cisco Catalyst 9120 AP reloads unexpectedly due to radio firmware crash.
CSCwc49970	Channel 165 is not allowed in Cisco Aironet 2800, 3800, and 4800 Series APs.
CSCwf22246	Cisco Catalyst 9130 AP does not include the management frame count calculation across AP chipsets.
CSCwf92148	Cisco Catalyst 9120 AP does not disable High Efficiency with dual 5-GHz in Slot 0.
CSCwd60034	Cisco Aironet 3800 AP radio reloads unexpectedly when beacon is stuck.
CSCwe12057	Controller Quality of Service (QoS) page does not load when ACL has double quotes as special character in the name.
CSCwd98332	Controller crashes after failing to match the interface ID in the anchor message.
CSCvz26009	Cisco Catalyst 9800-CL Wireless Controller allocates only 256-MB of DRAM or EXMEM leading to instability and CPP crashes.
CSCwe84267	Cisco Catalyst 9115 AP does not transmit the first CAPWAP data keepalive on wire during N+1 failover in FlexConnect mode.
CSCwe49267	Controller does not send the group temporal key (GTK) M5 packet to Cisco IP Phone 8821 after Fast Transition roaming between wncds.
CSCwf32342	Client is unable to roam successfully and pass traffic in SDA environment.
CSCwf83278	Client traffic fails with N+1 when Cisco Catalyst 9120 AP sends CLIENT_DEL_STOP_REASSOC.
CSCwe67580	CAWAP tunnel is not formed between Office Extend Access Points (OEAP) and controller after changing the public IP.
CSCwd49166	Cisco Aironet 3800 AP consistently reports high QoS Basic Set Service (QBSS) load.
CSCwf11117	Cisco Catalyst 9120 AP deauthenticates the WGB continuously after roam.
CSCwf71906	Controller does not plumb IPv4 address in IP Source Guard (IPSG) datapath in CWA SSIDs for clients with single IPv4 address.
CSCwf24468	The **show wireless client detail sum** command displays Apple iPad (10 generation) as not classified and unknown device.

Identifier	Headline
CSCwd63516	Cisco Catalyst 9120 AP fails the EAP-TLS port authentication as password cannot be decrypted.
CSCwd83840	Cisco Aironet 1830 AP fails with **writing to fd 27 failed!** error when connecting to the controller.
CSCwd52745	Cisco Aironet 3802 AP experiences kernel crash.
CSCwe19858	Cisco Catalyst 9130 AP displays incorrect **Local power constraint** value in management frames.
CSCwd77188	Cisco Aironet 3802 AP broadcasts different power values in beacon country IE.
CSCwf68131	Cisco Catalyst 9105AXW AP fails to boot when number of bad blocks are greater than 90.
CSCwd95618	The **device-tracking binding reachable-lifetime** command does not work on the controller.
CSCwb72924	Client in FlexConnect mode is unable to reconnect to an AP.
CSCwe91394	Aeroscout T15e (Third-party device) tags attached to medical devices do not report temperature data due to extra bytes. Apple
CSCwf77030	CSV file import fails when static AP mapping table already contains few entries.
CSCwf07384	Wired client behind Cisco Catalyst 9105 AP fails to pass traffic.
CSCwf57471	Controller GUI hangs when Application Visibility and Control (AVC) profile is enabled with special characters.
CSCwf65794	Cisco Aironet 1852 AP crashes due to radio failure.
CSCwd77823	Cisco Catalyst 9130 AP experiences random radio firmware reload.
CSCwf07264	WNCd crash is observed when accessing Crimson database.
CSCwe45553	One-shot error is displayed when applying AP Service Pack (APSP) on controller.
CSCwe67810	Cisco Wave 2 APs in FlexConnect standalone mode experiences client disconnections.
CSCwe55390	Spectralink Versity 9553 phones experience sporadic and robotic voice delays during a short period after Fast Transition roaming between Cisco Aironet 3802 APs.
CSCwe18185	Cisco Catalyst 9130 (VID03) AP does not have the "iox.tar.gz" file in Day 0 factory image.
CSCwd07298	Higher packet loss is observed during Cisco IP Phone 8821 voice call.
CSCwf88890	The **Monitoring** > **Wireless** > **AP Statistics** page does not load in the GUI for Cisco Aironet 3800 AP.

Identifier	Headline
CSCwd90472	Wireless device tracking fails while adding static IP and MAC bindings.
CSCwf76119	Clients after a Change of Authorization (CoA) is allowed network access for a short duration using cached PMK.
CSCwd79645	Wireless client cannot communicate after session timeout when AP drops once during the session.
CSCwe71996	Associated APs are not seen in Cisco DNAC.
CSCwe22625	Controller GUI login screen appears blank when ampersand is used in username.
CSCwb51757	Access Points intermittently report high channel usage in 5-GHz radio with 40 MHz.
CSCwf52815	Cisco Wave 2 APs improve PMTU discovery mechanism to honor the ICMP unreachable maximum transmission unit (MTU) value.
CSCwf55303	Active controller reboots when redundancy port (RP) link comes up.
CSCwd56391	Controller does not provide RSSI location data for some of the RFID tags in database.
CSCwe00848	Cisco Catalyst 9105 AP randomly reloads with **Kernel panic - not syncing: Fatal exception** error message.
CSCwe92340	Cisco Catalyst 9136i AP crashes due to kernel panic.
CSCwe15172	The image download space check in /tmp is 40 MB only, most of the AP image has more than 60 MB.
CSCwe96206	Clients are unable to roam between APs with WPA3 enterprise SSID and SuiteB192.
CSCwf40430	Mobile devices cannot prompt incorrect password in Cisco Catalyst 9130 AP or controller after PSK SSID password is changed.
CSCwe92462	Client data rate displays greater value in Assurance Client dashboard.
CSCwe85742	Controller clears PMK ID when it fails to ressurect client entry upon N+1 AP failover.
CSCwf31925	Controller does not send reassociation response for Fast Transition reassociation request with RIC for TID 0.
CSCwa93884	Cisco IOx application experiences installation failure during application activation phase.
CSCwd36552	Cisco Catalyst 9120 AP reloads unexpectedly with the following error message: "kernel panic - not syncing: fatal exception"
CSCwe30473	Cisco Wave 2 APs radio firmware reloads unexpectedly when queue is stuck.
CSCwe52756	Cisco Catalyst 9120 AP sends RTS with 6 Mbps when the rate is configured as unsupported.

Identifier	Headline
CSCwe82287	AP does not allow a PMF WPA3 client to associate after the client sends deauthentication by itself.
CSCwe30572	Cisco Wave 2 APs leak Network Address Translation (NAT) IP from Cisco IOx application.
CSCwf28105	Cisco Catalyst 9130AX AP experiences kernel panic.
CSCwd91054	Cisco Wave 2 APs are not encrypting EAP_ID_REQ after M1 to M4 and not updating PMKID for dot1x OKC.
CSCwf94863	Cisco Catalyst 9115 AP experiences kernel panic when PC or LR is at drop_pagecache_sb+0x78/0x110.
CSCwf54827	Wireless client is deauthenticated after idle timeout.
CSCwf95868	Single band BCM WGB radio 0 transmission power decrease by nearly 20 dBm while configuring the antenna number.
CSCwe91264	AP crashes when PC and LR are at get_partial_node.isra.
CSCwf28550	Controller and Cisco Catalyst 9124 AP are unable to get wired client information from workgroup bridge.
CSCwe07802	Cisco Wave 2 APs drop upstream Extensible Authentication Protocol (EAP) packets.
CSCwe91371	Cisco Catalyst 9130 AP does not transmit beacons.
CSCwe18012	Crash is observed in the standby controller when saving QOS table to standby.
CSCwe17920	Cisco Catalyst 9124 AP does not forward traffic to workgroup bridge after a session timeout.
CSCwa16835	Wireless traffic encapsulated in VXLAN from AP to FE is dropped when the destination MAC is incorrect.
CSCwa36515	The following syslog message is displayed while changing AP location using controller GUI: **% Error: AP is already in the requested state**
CSCwe70970	Need an option to prioritize keepalives in the RP port in the HA-SSO deployment.
CSCwf44027	The username is missing randomly for wireless 802.1x clients.
CSCwd41463	AP intermittently stops sending Internet Group Management Protocol (IGMP) membership report.
CSCwf50177	Cisco Catalyst 9105AXW AP experiences large number of bad blocks.
CSCwf04748	AP crashes due to CALLBACK FULL reset radio error.
CSCwd88150	Root certificates of CG522E are lost after each reload.

Identifier	Headline
CSCwf71255	The client traffic stops after the AP fails over to N+1 controller with FlexConnect local switching.
CSCwe42302	Cisco Catalyst 9800 Wireless Controller Inter-Release Controller Mobility (IRCM) client is deleted due to profile name mismatch.
CSCwa86015	Cisco Catalyst 9120 Series AP experiences kernel panic crash.
CSCwf54714	Controller reloads unexpectedly.
CSCwd08068	Cisco Aironet 1815W AP crashes due to out-of-memory issue.
CSCwd35577	Redundancy fails during double bit ECC error.
CSCwd03205	WGB wired clients connected to RAP in local mode, sends upstream broadcast packets and causes out-of-memory on the RAP.
CSCwf42824	Cisco Catalyst 9105AXW Series APs do not recover after upgrade.
CSCwe87973	Cisco Aironet 3800 Series AP reloads unexpectedly due to FIQ/NMI reset.
CSCwd46815	Cisco Aironet 2800/3800/4800/1562 Series APs and Cisco Catalyst IW6300 Heavy Duty Series APs: EAP-TLS fails for wired clients behind MAP.
CSCwf87904	Cisco Catalyst 9164 Series AP randomly crashes and restarts.
CSCwe30429	Cisco Catalyst 9800-L wireless controller shows "Last reload reason: reload" instead of "Critical process wncd fault".
CSCwf25869	Radio core crashes due to TCQ stuck state with frequent channel changes.
CSCwf32806	Controller reloads unexpectedly with the following message: "Critical process wncd fault on rp_0_0 (rc=134)"
CSCwe82892	Clients connected to FlexConnect AP with profile policy is assigned to VLAN ID=1 instead of native VLAN.
CSCwe62694	Controller EVENTLIB-3-CPUHOG Traceback is observed.
CSCwd99656	The **snmp-server host** command does filter special characters effectively.
CSCwe32853	Cisco Catalyst 9124AXI AP does not forward RLAN traffic to the upstream network.
CSCwe25446	Unexpected reboot due to Wireless Network Control Daemon (WNCD).
CSCwe04602	Cisco Wave 2 APs fail to forward traffic to wireless clients for about 60 seconds in SDA fabric WLANs.
CSCwe73403	DHCP Option 82 is not added in WLAN with EoGRE tunnel when SVI interface is down.
CSCwe35906	Radio firmware crash experienced in Cisco Catalyst 9117 Series AP.

Identifier	Headline
CSCwe74874	Cisco Catalyst 9120 Series AP experiences kernel panic.
CSCwf21311	Cisco Catalyst 9166D1 AP crashes due to kclick.
CSCwf13445	Reliable Multicast (MC2UC) does not work for controller, Cisco Industrial Wireless 3702 Series Access Point, and Cisco Industrial Wireless 3700 Series Access Point WGB for native VLAN.
CSCwf87281	Segmentation fault on the controller due to NULL timer.
CSCwh17592	Cisco Catalyst 9130AXI Series AP Slot 1 does not announce High Throughput (HT)/Very High Throughput (VHT)/High-Efficiency (HE) capabilities when dual radio is enabled.
CSCwe76818	Syslog configuration does not reflect in the Cisco Aironet 3800 AP.
CSCwe76817	Cisco Wave 2 AP logs display CAPWAP MTU discovery issues.
CSCwd68141	Rogue containment details are not shown in the **show wireless wps rogue ap detail** command.
CSCwe01579	WNCD process crashes unexpectedly in a large scale setup.
CSCwe66730	Dynamic Channel Assignment (DCA) assigns wrong channels after Dynamic Frequency Selection (DFS) events.
CSCwe35285	EAP ID request is not sent from AP to client.
CSCwf13879	Cisco Catalyst 9800-CL Wireless Controller crashes unexpectedly.
CSCwf88588	ISSU upgrade causes AP Manager to crash and controller to go on boot loop.
CSCwf09008	Cisco Catalyst 9800-CL Wireless Controller crashes with the following error message: "Last reload reason: Critical process wncd fault on rp_0_0 (rc=139)".
CSCwf62051	Cisco Aironet 1815W AP crashes due to kernel panic.
CSCwh35072	Cisco Aironet 3800 Series AP reloads unexpectedly due to FIQ/NMI reset.
CSCwe27839	Kernel panic observed on Cisco Catalyst 9120 Series AP.
CSCwe80617	Wireless clients are unable to connect to Cisco Aironet 1830 Series AP after an input or output error message.
CSCwd86288	Load average warning messages are displayed when Cisco Catalyst 9800-80 Wireless Controller is healthy.
CSCwf44483	The 5-GHz radio is operationally down in the -A domain APs in Panama.
CSCwd46770	Controller License: Remove Reporting Interval (which is fixed to 8 hours) and change Sync Report to user action.

Identifier	Headline
CSCwf90646	Controller sends two CAPWAP control payloads for DOT11R_WLC_MAC_IP_PAYLOAD with the same sequence numbers.
CSCwd74571	WCPd crashes unexpectedly due to reuse of freed packets.
CSCwd96376	Unable to login to the controller GUI or command line interface with a user created by Day 0 wizard.
CSCwf09259	AP LED flash automatically turns on after reboot.
CSCwf67316	AP may not detect radar on the required levels after CAC time.
CSCwd49861	Controller OID documentation is incomplete in the MIB file.
CSCwe63089	LED on APs turning white randomly.
CSCwf22225	Cisco Catalyst 9120 Series AP: Probes and beacons are not included in the management frame count across AP chipsets.
CSCwe74895	Controller crashes when running AP packet capture.
CSCwe15338	Cisco Catalyst 9120 Series AP does not respond to client's probe or authentication due to the TX STUCK issue.
CSCwf12104	Unable to downgrade the Cisco Cellular Gateway device through the vManage GUI.
CSCwh08625	Cisco Catalyst 9120 Series AP experiences kernel panic crash.
CSCwe14729	Controller reboots due to memory corruption when processing DHCP Option 82.
CSCwd79502	Controller device tracks stale entry due to the anchored client receiving IPv4 and IPv6 in different VLANs.
CSCwe71081	Login error observed in macOS with guest login.
CSCwe38480	The controller EPC inner filter captures CAPWAP data fragments and CAPWAP control not filtered by MAC.
CSCwe87845	Cisco Industrial Wireless 3702 Series AP's WGB changes TID for EAP packets from TID 7 to TID 0.
CSCwf15582	Cisco Wave 2 AP radio reloads unexpectedly due to the beacon being stuck.
CSCwf75646	Controller MIB files do not include all coded integer values.
CSCwf45495	Cisco Catalyst 9130 Series APs fail to start CAPWAP due to interface reset every 52 seconds, during the DHCP process.
CSCwf53130	Cisco Catalyst 9166 Series AP crashes and leaves the crash file in the controller.
CSCwf86242	The controller reloads unexpectedly with CAPWAP window size set to 0.
CSCwe95127	The controller provides incorrect data for certain APs in response to the SNMP query bsnAPIfDot11BSSID.

Identifier	Headline
CSCwf29742	Cisco Catalyst 9120 Series AP: Firmware crashes when running multicast and longevity with more than 80 clients.
CSCwf64009	Cisco Aironet 1815 Series AP drops RLAN and VLAN traffic with looped port.
CSCwe74653	Cisco Wave 2 APs do not send the delete reason to the controller, resulting in stale entries.
CSCwf63818	Kernal panic crash observed on Cisco Aironet 1830 Series AP.
CSCwf07605	Cisco Catalyst 9105 Series AP and Cisco Aironet 1815 Series AP MAC device cannot get an IP address in the Ethernet port after AAA VLAN override.
CSCwc75732	Cisco Aironet 4800 AP FW crash is observed in Radio 1.
CSCwd81523	Cisco Catalyst 9130 Series AP do not send EAP_ID_RESP after PMF client TX deauthentication, in the middle of EAP handshake.
CSCwe99957	The controller does not respond to keepalives from the AP after AP disconnect.
CSCwh20934	Cisco Wave 2 AP reloads due to Systemd critical process crash.
CSCwe70039	Clients are stuck in an authentication loop after N+1 HA switchover.
CSCwe11547	RRM process crashes on the controller.
CSCwd59921	Cisco Catalyst 9130 Series AP drops EAP-TLS frames.
CSCwc70256	Cisco Catalyst 9166 Series AP: Kernel panic or crash observed.

Resolved Caveats for Cisco IOS XE, Bengaluru, 17.6.5

Caveat ID	Description
CSCvv96364	WCPd crash is seen on Cisco Aironet 3800 APs.
CSCvx32806	Cisco Wave1 APs are stuck in bootup loop due to image checksum verification failure.
CSCvx80422	AP drops packets addressed to 10.128.128.127 or 10.128.128.128.
CSCvy53756	A pubd crash is observed in 200-AP mesh configuration with telemetry subscriptions.
CSCwa39598	iOX app fails to install on the Cisco Catalyst 9130, 9120, and Cisco Aironet 4800 APs.
CSCwa86610	Cisco Aironet 2802 and 3802 APs are crashing due to kernel panic.
CSCwa98980	Controller crashes in WNCd process when handling an EAP-NAK.

Caveat ID	Description
CSCwb07001	Cisco Catalyst 9166I AP in FlexConnect local-auth mode keeps rebooting when Federal Information Processing Standard (FIPS) is enabled with dot1x security client.
CSCwb15031	Client is not able to pass traffic after roaming using Wi-Fi Protected Access Version 2 (WPA2) Opportunistic Key Caching (OKC).
CSCwb78191	AAA VLAN override is not considered during Identity PSK (iPSK) authentication and anchor WLAN.
CSCwb79827	Controller ucode crashes due to CBAR/endpoint analytics.
CSCwb82694	Cisco Catalyst 9100 Series APs such as 9105, 9115, and 9120 are unable to handle out of order packets.
CSCwb96560	AppHost: App install fails when USB state is disabled in ap-join profile.
CSCwc05350	Cisco Wave 2 APs: CAPWAP maximum transmission unit (MTU) flaps due to asymmetric MTU from AP to controller and vice versa.
CSCwc05366	Wireless AAA Dynamic VLAN Assignment: Wireless clients cannot reach each other.
CSCwc15533	Continuous wncmgrd CPUHOG traceback with scale Flexible NetFlow (FNF) mapping to policy profile 100% WNCd utilization.
CSCwc15898	Cisco Catalyst 9120 and 9130 APs: CleanAir data for 2.4-GHz is missing.
CSCwc15944	Multicast data is not sent to clients; some APs unable to join.
CSCwc18004	PI is not displaying/process AP disassociate snmp-trap from controller.
CSCwc24994	Cisco Aironet 3800 AP crashes due to kernel panic.
CSCwc26819	Controller is not sending Logical Link Control (LLC) or XID spoofed frames after a mobility event.
CSCwc28408	WNCd crash on co_fetch_mbssid_from_rbssid.
CSCwc31331	Cisco Catalyst 9130 AP unexpectedly reloads.
CSCwc36910	cEdge device pushes wrong syntax.
CSCwc38912	Local Web Authentication (LWA) client is immediately deleted when joining FlexConnect WLAN after a change in site tag or policy tag.
CSCwc42784	Client fails to connect when protocol based QoS is configured.
CSCwc51894	Cisco Catalyst 9117 AP reloads unexpectedly due to kernel panic.

Caveat ID	Description
CSCwc54410	High Availability: Dual active scenario is observed when standby is reconnecting to HA pair.
CSCwc55153	Packet destined for Layer2 socket application gets delivered to Layer3 socket application.
CSCwc55632	Cisco Catalyst 9124 MAP is failing to connect to Cisco Aironet 1562 RAP after first reload of MAP.
CSCwc55982	Stale entry is observed in the **show wireless device tracking database ip** command output after client deletion.
CSCwc56707	CG522-E status on gateway and vManage is not synchronized. vManage is not showing the cellular statistics.
CSCwc56774	A WGB with static IP loses its IP address after multiple roams.
CSCwc57227	Controller WNCd crash is observed.
CSCwc59518	Cisco Catalyst 9800-80 controller crashes with the reason: Critical process WNCd fault on rp_0_3 (rc=134).
CSCwc68682	Link goes down due to local fault.
CSCwc71198	CAPWAP flap occurs when Virtual Router Redundancy Protocol (VRRP) version3 is present in the network.
CSCwc72194	Cisco Catalyst 9120 AP: Radio core dump is observed.
CSCwc73462	In FlexConnect groups configuration, backslash(\) at the end of the shared secret (for Radius servers) is not allowed.
CSCwc75102	AP conversion to CAPWAP via DHCP Option 43 is not working.
CSCwc78435	Cisco Catalyst 9130 AP is sending incorrect channel list on out of band Dynamic Frequency Selection (DFS) event causing client connectivity issues.
CSCwc81341	Cisco Catalyst 9130 AP: Kernel panic crash is observed with memory corruption with ICAP.
CSCwc87688	Cisco Catalyst 9120 AP shows high noise levels on 5-GHz radio.
CSCwc89183	Controller crashes on libewlc_client_dpath_svc.so.
CSCwc89719	Cisco Aironet 1832 AP crashes due to radio failure.
CSCwc93198	Cisco Catalyst 9800-L controller is not getting HWDIB down message when RP port goes down in HA. Resultantly, Gratuitous ARP (GARP) is not sent from WMI.
CSCwc94898	A workgroup bridge (WGB) AP is stuck in Extensible Authentication Protocol over LAN (EAPOL) state.

Caveat ID	Description
CSCwc96683	Cisco Wave1 APs n FlexConnect local-switching mode is not forwarding IP fragmented packets received with DF.
CSCwd00751	Cisco Aironet 2802 AP crash is observed.
CSCwd02898	Cisco Catalyst 9300 switch is not flushing remote MAC address after roaming to a local AP.
CSCwd03803	Cisco Aironet 1815I AP is rebooting -PC is at edma_poll / LR is at dma_cache_maint_page
CSCwd04025	PI 3.10.1: APs associated with controller is showing interface as \"Half duplex\".
CSCwd04571	Memory leak is observed in wncd process when under load.
CSCwd06001	Linux IOSd crash is observed on standby controller during reload of the Cisco Catalyst 9800-L controller.
CSCwd06018	802.11r re-auth failed due to invalid Pairwise Master Key ID (PMKID) while doing inter-WNCd roaming.
CSCwd06122	AP join issues observed due to stale client entries.
CSCwd08165	Controller is accounting wrong class attribute in accounting packets.
CSCwd08259	Cisco Catalyst 9120, 9115, and 9105 APs: Radio firmware crash is observed.
CSCwd08678	Timer is not running; stale client are not deleted by the controller.
CSCwd10570	Cisco Catalyst 9130 AP sends beacon with incorrect datarates; different rates are sent for same slot on different BSSIDs.
CSCwd12135	IOS-XE crash on Pubd core@green_be_rec_marshal_inline while removing or adding telemetry server hostname.
CSCwd17349	Active chassis might get stuck during the SSO failover.
CSCwd19631	Cisco Catalyst 9120 AP cannot operate in mGig when EEE is enabled on switchport.
CSCwd21996	Cisco Catalyst 9120 AP: CleanAir sensor is crashing.
CSCwd23681	Controller fails to update AP configuration with error \"% Error: no ap_name exists\".
CSCwd24275	IPReassembler element strips last 20 bytes of last fragment.
CSCwd32107	Ignore CAPWAP_PAYLOAD: AP_LAN_CONFIG payload has wrong RLAN port enable value from Cisco Aironet 2700 AP.

Caveat ID	Description
CSCwd34890	Clients are getting deauthenticated imediately after getting IP address in a configuration that has local web authentication + local switching + central authetication.
CSCwd35393	Wireless load-balancing affinity incorrectly shows AP site tag as default-site.
CSCwd38069	Multicast Domain Name System (mDNS)-gw Location Specific Services (LSS) is not filtering correctly if AP with services and Radio Resource Management (RRM) neighbor radio start 00XX.
CSCwd39605	Cisco Catalyst 9117 AP reloads unexpectedly due to kernel panic.
CSCwd40731	AP reloads due to kernel panic.
CSCwd46091	Cisco Catalyst 9105AXI AP is requesting 30 watts of power instead of 15.4 watts.
CSCwd46721	IP theft occurs due to client stale entries in ODM database.
CSCwd48118	AP saves only 31 characters instead of 32 for site tag causing the AP to go into misconfiguration state.
CSCwd52385	AP is not initiating Google Remote Procedure Calls (gRPC) connection to Cisco DNA Centre correctly after token expiry.
CSCwd55757	Wave 2 APs are crashing: Systemd critical process crash - dnsmasq-host.service failed.
CSCwd60376	Cisco Catalyst 9120 AP: Kernel panic is observed.
CSCwd63665	Cisco Catalyst 9800-80 controller shows consistent high CPU utilization in WNCd with 200 APs.
CSCwd63861	SIGSEGV crash is observed when incrementing roaming statistics.
CSCwd80290	AP image validation certificate is either failed or expired, causing AP join issues.

Resolved Caveats for Cisco IOS XE, Bengaluru, 17.6.4

Caveat ID	Description
CSCwb99144	Controller reloads unexpectedly due to Multicast Domain Name System (mDNS).
CSCwa09693	PMK-Propagation bulk sync failures are observed with scaled setup.
CSCwa10377	Cisco Catalyst 9800-80 Controller in SSO running Cisco IOS XE 17.3.4 with APSP and SMU crashes causing unexpected High Availability failure.

Caveat ID	Description
CSCwa50929	Controller goes fore crash within 10 minutes after starting pure intra wnc roam at 600 clients per second.
CSCwa67566	Controller rejects clients with wrong PMKID when changing Authenticated Key Management (AKM) from Fast Transition (FT) to dot1x and vice-versa.
CSCwa69631	Controller reloads unexpectedly when WebAuth AAA routines generate WNCd core.
CSCwa70649	Improve serviceability to figure out the reason as to why the controller blacklists 802.11w client.
CSCwa70852	WNCd crash is observed while handling Protected Management Frame (PMF) action for Intel client.
CSCwa77214	Controller crashes at ewlc_wlanmgr_wlan_ref_count_cleanup_timer_cb.
CSCwa79968	SNMP MIB at times does not return all data or no data at all for SNMP walk with high client count.
CSCwa88790	Controller crashes during mobility routines generating WNCd core.
CSCwa99904	Controller deletes client when DHCP RELEASE is sent by client during posture.
CSCwb05014	Controller experiences repeated crashes in WNCd process when changing **mac ip binding** configuration.
CSCwb09214	Controller sends QBSS_AAC with zero available bandwidth for several seconds after DEL TS.
CSCwb17255	WNCD platform state displays as DEAD for **show aaa servers** output.
CSCwb21141	WLANs do not get pushed to APs in a single instance because **wlan status** is not updated and remains FALSE.
CSCwb24037	Client gets stuck in **Authenticating** state after failing GTK broadcast rotation.
CSCwb27940	Client gets deleted due to VLAN failure after performing L3 roaming if VLAN persistency is enabled.
CSCwb29197	WNCd crash is observed in scale scenario where IDMGR IDs are exhaustively used.
CSCwb31335	Standby controller goes to standby recovery when **Gateway Failover** toggle button is enabled.
CSCwb35196	High CPU utilization in WNCd due to continuous log in ra_trace "WebAuth info not found while termin".

Caveat ID	Description
CSCwb37940	Controller blacklists 802.11w client due to **CO_CLIENT_DELETE_REASON_EXCLUDE_VLAN_FAIL**.
CSCwb39307	AAA server does not mark as UP even when it is reachable and client does not get authenticated using this server.
CSCwb42717	WNCd process crashes when CAPWAP multi-window feature is enabled.
CSCwb45089	HTTPS access to the controller is broken after an upgrade to Cisco IOS XE 17.3.5a.
CSCwb57391	Client gets disassociated with **CO_CLIENT_DELETE_REASON_IP_DOWN_NO_IP** reason when client roams from one AP to another.
CSCwb65356	Controller reloads with the **Critical process wncd fault on rp_0_0 (rc=139)** reason.
CSCwb69531	Controller initiates Extensible Authentication Protocol over LAN (EAPOL) reties for the client in **RUN** state.
CSCwb73136	Clients are unable to pass traffic in RUN state after CoA is completed.
CSCwb80500	WNCD process experiences memory leak due to unknown responses from the RADIUS server.
CSCwc01644	COS AP assigns Flex local switching clients to the native VLAN instead of the VLAN selected in the Policy Profile.
CSCwc04197	Secondary controller crashes during redundancy switchover.
CSCwc32226	Zebra RF Gun clients are deleted randomly from the controller due to **CO_CLIENT_DELETE_REASON_ZONE_CHANGE**.
CSCvy37351	Telemetry data is not being sent from the controller for few tens of seconds at high scale.
CSCwa38847	CCO download works with CISCO account but not with guest account.
CSCwa74884	Controller sends the wrong payload information to AP when mesh RRM is enabled or disabled.
CSCwa87435	Controller sends duplicate NS frame as unicast to wireless client or WGB and blocks the duplicate address detection (DAD) process.
CSCwa91689	Logging message is not seen when load profile threshold is moved to passed or failed for 2.4GHz radio.
CSCwa95336	Static workgroup bridge (WGB) client does not move to RUN state in the controller.

Caveat ID	Description
CSCwb05825	MAC authentication bypass (MAB) client does not move to the exclude state during a MAB failure.
CSCwb15884	Memory depletion and high Wide Area Network (WAN) latency is observed in FlexConnect deployment.
CSCwb22867	WNCD process crashes when applying Air Time Fairness (ATF) profiles.
CSCwb35761	Incorrect VLAN is assigned to initiate SIP when SIP and AAA override combination is used.
CSCwb37457	Standby controller crashes when controller is configured in RMI + RP High Availability mode with wired guest feature.
CSCwb43261	Packets drop in Cisco Catalyst 9800-CL or 9800-L Wireless Controller when call snooping and SIP CAC is enabled.
CSCwb45637	Samsung devices with more than 1 character Country code do not get classified properly.
CSCwb63861	**wireless wlan clear-refcount** command does not accept WLAN or policy names with special characters.
CSCwb64761	Controller discards location updates from radio frequency identification (RFID) tags.
CSCwb67450	The **show process cpu platform sorted** command is critical to monitor some Cisco Catalyst 9800 Series Wireless Controller platform issues.
CSCwb87440	Controller can end with SN values different than the Cisco standard ones.
CSCwb93513	Stale client entries are not deleted automatically nor by clear commands and stuck on device-tracking database.
CSCwc38828	Invalid TDL pointers cause WNCd crash in controller.
CSCwa06456	Cisco Catalyst 9130 AP radio experiences a radioFW crash causing network down.
CSCwa08478	Cisco Aironet 4800 AP crash core file observed after 4 days uptime with console message: '[cmd timeout] wifi0: 0x9201=GetRadioStatus'.
CSCwa26814	Cisco Aironet 3800 AP does not pass ARP requests on central WLAN when configured in Custom Flex Group.
CSCwa42620	Cisco Catalyst 9130 APs drop traffic on air for Phoenix WinNonlin application.

Caveat ID	Description
CSCwa54943	COS APs with RLAN port connecting to the device running LLDP reboots due to Out of Memory.
CSCwa65318	Transmission power for slot2 is set to the lowest power level (-2dbm or -4dbm) due to which clients are unable to join.
CSCwa68439	Cisco Aironet 3800 AP sends a burst of deauthentication frames after each session timeout for each AP in PSK WLAN.
CSCwa75901	Radio recovery fails when Cisco Catalyst 9117 beacon is stuck.
CSCwa77205	Cisco Aironet 1832, 1852, and 1815 experiences Kernel Panic at **wlan_handle_napi**.
CSCwa88621	Cisco Catalyst 9120AXI AP - capwapd.service failed.
CSCwa90871	Cisco Catalyst 9120 AP running Cisco IOS XE 17.7.1.11 experiences software crash in wcpd process.
CSCwa96198	Central Web Authentication (CWA) clients with Run state cannot go online even though it is in Run state.
CSCwa96429	COS AP disconnects from the controller after CTS switchport configuration.
CSCwb05556	AP does not send multicast data till it snoops IGMPv2.
CSCwb08755	Cisco Catalyst 9130 or 9120 AP in FlexConnect mode does not send Security Association (SA) query.
CSCwb09248	High latency and drops observed when associated with Cisco Catalyst 9130 AP.
CSCwb11711	Cisco Catalyst 9120 or 9130 APs in FlexConnect send Association reject after first successful connection.
CSCwb19448	Cisco Catalyst 9117 AP crashes due to kernel panic in **cisco_wlan_crypto_decap**.
CSCwb23976	Cisco Catalyst 9117 AP crashes due to Kernel Panic **dp_print_host_stats**.
CSCwb28006	Cisco Aironet 3800 AP plumbs client to VLAN 1 instead of native VLAN 0 causing ARP drops **OUTER_UCAST_VLAN_BLOCK**.
CSCwb30993	Cisco Catalyst 9117AXI-E AP experiences kernel panic crashes.
CSCwb32121	Cisco Aironet 1832 AP reloads due to radio failure - Beacon Stuck-reset radio for recovery.
CSCwb36531	Cisco Catalyst 9130 AP is unable to process fragmented EAP frames from client when performing EAP-TLS.

Caveat ID	Description
CSCwb38948	Cisco Catalyst 9124 AP: Sometime MAPs are no longer able to join RAP for security failures.
CSCwb53348	Cisco Catalyst 9130 APs generate radio coredumps.
CSCwb68720	AP sends the address resolution protocol (ARP) packet without VXLAN encapsulation.
CSCwb70757	Cisco Catalyst 9130 AP crashes due to kernel panic.
CSCwb91830	Possible radio reset loop when bootup.
CSCwb93281	Cisco Catalyst 9130 AP crashes due to dp_soc_deinit_wifi3+0x354/0x3c0.
CSCwb94209	Mode reset button does not clear CC mode and console blocking configuration in Cisco Catalyst 9115 AP.
CSCwb95980	Cisco Catalyst 9130 AP Kernal crash - PC is at _ZN10CACMetrics25accumulate.
CSCwc03853	SJC24 Alpha Cisco Catalyst 9105 OEAP RLAN1 poe stopped working in Cisco IOS XE 17.9.0.115.
CSCwc09461	Cisco Catalyst 9120 APs delay authentication response frame.
CSCwc15229	Cisco Aironet 1832 AP reloads due to radio failure - Beacons stuck in radio.
CSCwc20929	APP-hosting segmentation does not work in Cisco Catalyst 9100 AP or Cisco Catalyst 9800 Series Wireless Controller and Cisco IOS XE 17.6.3.
CSCvx51916	Cisco Catalyst 9120 AP displays **ASLR ENTROPY INSUFFICIENT** messages.
CSCvz90902	Cisco Catalyst 9130 AP Probe suppression for Macro-Micro cell client steering does not work.
CSCwa33537	Cisco Catalyst 9117AX AP radio reloads unexpectedly due to partial command issues.
CSCwa48648	Wireless devices receive Invalid Fast Transition (FT) IE when using FT over-the-ds to roam.
CSCwa53727	Cisco Catalyst 9117AX AP reloads unexpectedly at cmnos_thread.c:3493.
CSCwa61087	Cisco Aironet 1562 AP acting as WGB is unable to pass multicast traffic to the passive client behind it.
CSCwa72688	Template attach fails when using authentication type NONE for profile.

Caveat ID	Description
CSCwa73535	Cisco Aironet 1830 or 1850 AP does not advertise HT/VHT IE in beacons or probes without the custom channel width change.
CSCwa73820	Cisco Aironet 4800 AP does not negotiate full power using LLDP.
CSCwa76008	The "Channel Center Segment 0" value in " VHT Operation Info" is set to "0" using Cisco Aironet 2802 AP.
CSCwa77633	Cisco Aironet 1832 AP crashes due to kernel panic.
CSCwa79564	Power Type is displayed incorrectly for Cisco Aironet 2800 or 3800 APs when static power is set to 15.4W.
CSCwa84149	PROFINET multicast traffic is dropped in Flex + Bridge and local switching modes.
CSCwa85088	Wired client behind Cisco WGB does not take the DHCP IP address.
CSCwa95705	Cisco Aironet 2802 AP reloads unexpectedly due to FIQ or NMI reset.
CSCwb08956	Cisco Aironet 2800 APs change the Traffic Identifier (TID) for EAPOL packets from 6 to 0 after changing the RF profile in the controller.
CSCwb11854	Low Throughput is observed with Cisco 8540 Wireless Controller and Cisco Aironet 1852 AP.
CSCwb15328	Kernel panic is observed at wlc_fifo_index_peek+0x68/0xa0 [wl].
CSCwb16086	Kernel panic is observed at ieee80211_bsscolor_update_bsscolor_list.
CSCwb19680	Incorrect kernel assertion in checking invalid timer objects.
CSCwb19993	Cisco Aironet 1852 AP loses configuration after an upgrade.
CSCwb45599	AP crash is observed when PC is at ppr_create_prealloc+0xbc.
CSCwb73294	Cisco Catalyst 9105 AP displays low throughput in 2.4GHz with AX clients and adjacent channel interference.
CSCwb76882	Cisco Catalyst 9130 AP detects its own BSSID as Rogue in 5GHz channel.
CSCwb90245	Cisco Catalyst 9120 AP radio dumps core.
CSCwb98247	AP crash observed in wlan_objmgr_peer_release_ref running Cisco IOS XE 17.3.5.
CSCwc04079	COS AP in WGB mode is unable to assign static IP with subnet mask other than /24.

Caveat ID	Description
CSCwc07002	AP crash kernel panic is observed at pci_generic_config_read.
CSCwb25655	Functional SJC Cisco Catalyst 9136i AP experiences gRPC crash in ap-17.8.0.112.
CSCwb51541	Cisco COS APs delay forwarding of upstream Fast Transition (FT)-Auth request frame to the controller.
CSCwc17012	Protected Management Frame (PMF) clients are not able to connect to IOS APs when PMF optional or mandatory configured AP is not replying to assoc-request.
CSCwc35321	Cisco COS APs in Local mode sends Address Resolution Protocol (ARP) requests to wireless clients from 10.128.128.128 IP address.
CSCwb07125	APs own MAC is detected as rogue in slot1 or slot3 intermittently with an empty SSID.

Resolved Caveats for Cisco IOS XE, Bengaluru, 17.6.3

Caveat ID	Description
CSCvi48253	Self-signed certificates cannot be created after 00:00 1 Jan 2020 UTC.
CSCwa24836	Cisco Catalyst 9120 or 9130 AP leads to CAPWAP process crash loop when AP management password contains white spaces.
CSCvz34172	Cisco Aironet 1832 AP experiences kernel panic while setting client ACL in Cisco IOS-XE 17.3.4.
CSCvz59191	Cisco Catalyst 9120, 9130, and 9124 APs do not send NDP packets on slot 1.
CSCvz64295	Cisco Aironet 1815 AP FW assert issue is observed in Cisco IOS-XE 17.3.4 ES image.
CSCvz94267	Cisco Catalyst 9130 APs reload unexpectedly after upgrading to 17.3.4 and applying the ESW7 image.
CSCvz95465	Cisco Catalyst 9117 AP reloads unexpectedly due to kernel panic.
CSCvz99288	Cisco Catalyst 9130 AP reloads unexpectedly in Hostapd due to unhandled level 1 translation fault.
CSCwa06321	Change parameter in WLAN resets the Cisco Catalyst 9120 AP radio.
CSCwa08875	Cisco Aironet 3800 series AP crash due to kernel panic.
CSCwa15931	Cisco Catalyst 9124 AP experiences low SNR MAP disconnects with RAP when traffic is executed from MAP to RAP.

Caveat ID	Description
CSCwa18545	Cisco Catalyst 9120 AP starts beaconing with client TIM even when the client is replying to QoS Null.
CSCwa38125	Cisco Catalyst 9130 AP experiences kernel panic crash in monitor path.
CSCwa49981	Cisco Catalyst 9130 AP crashes due to frequent radio resets.
CSCwa52449	Cisco Catalyst 9117 AP experiences kernel panic crash at dp_rx_process.
CSCwa53266	Cisco Catalyst 9120 APs are unable to complete authentication and get stuck when 802.11w clients join the APs.
CSCwa73245	Cisco Aironet 3802 AP experiences MU sounding errors leading to TCQ stuck issue.
CSCwa73462	Cisco Aironet 1832 AP Indonesia is not beaconing as expected causing client performance issue.
CSCwa82660	Cisco Aironet 2800 or 3800 APs update only QBSS_AAC after radio reset and CAC configured.
CSCvu75017	Cisco Wave 2 and 802.11AX APs syslog is seen when using "Kern" facility value in AP join profile.
CSCvy60791	Dual Radio Assignment is missing for random Cisco Catalyst 9130AXI APs.
CSCvz40749	Probe filter in Cisco Catalyst 9120 AP does not limit unwanted probes from AP to the controller.
CSCvz69846	Cisco Aironet 2800 AP sends A-MSDU even after the client rejects it.
CSCvz79327	Cisco Aironet 1832 AP reloads unexpectedly due to radio failure (Beacon Stuck).
CSCvz89542	Enabling NAC on the policy profile breaks split tunnels in Cisco Catalyst 9105AX AP.
CSCvz95502	WGB wired clients cannot reach the standard gateway temporarily when MAC flapping occurs between the actual port and WGB switch port.
CSCvz99449	Identitymgmt service in Cisco DNA Center crashes when APs make too many connections to Identitymgmt.
CSCwa12278	Cisco Catalyst 9115 AP reloads unexpectedly due to kernel panic.
CSCwa24080	Client cannot connect to Cisco Catalyst 9130 AP with tri-radio (slot 2) enabled.

Caveat ID	Description
CSCwa35428	Cisco Catalyst 9120 AP drops CAPWAP connection when running the debug client.
CSCwa37641	Not able to discover and print using mDNS as SRV, TXT, A/AAAA records are removed based on TTL.
CSCwa44807	Cisco 9136 SW crashed on Process odhcp6c.
CSCwa48702	Cisco Catalyst 9130AX AP experiences kernel panic crash.
CSCwa49086	Cisco Aironet 3802 AP experiences FQI or NMI reset.
CSCwa49112	Cisco Aironet 3802 AP experiences FQI or NMI reset when PC is at loop_delay and LR is at wlRecv.
CSCwa49124	Cisco Aironet 3802 AP experiences kernel panic when PC is at _ZN19ProbeRequestTracker13simple_actionEP6Packet.
CSCwa49135	Cisco Aironet 3802 AP experiences kernel panic when PC is at sys_sigreturn and LR is at recalc_sigpending.
CSCwa53592	Cisco Catalyst 9120AX APs display Flexible Radio Assignment (FRA) not capable although FRA is enabled on Cisco IOS-XE 17.3.4c release.
CSCwa53745	Cisco Catalyst 9117AX AP reloads unexpectedly at whal_recv.c:629.
CSCwa53763	Cisco Catalyst 9117AX AP reloads unexpectedly at whal_xmit.c:3663.
CSCwa57078	Flap occurs between DHCP and static IP address when ethernet VLAN tagging is enabled on AP.
CSCwb08737	The comeback timer is missing when Cisco Catalyst 9130 or 9120 AP is configured in Flexconnect mode.
CSCwb08755	Cisco Catalyst 9130 or 9120 AP in FlexConnect mode does not send SA query.
CSCwb11711	Cisco Catalyst 9120 or 9130 APs in FlexConnect mode sends association reject after the first successful connection.
CSCwb19448	Cisco Catalyst 9117 AP crashes due to kernel panic in cisco_wlan_crypto_decap.
CSCwb20008	Cisco Catalyst 9130 AP driver crashes when PC and LR is at cnss_wlfw_wlan_cfg_send_sync.
CSCwb08291	Cisco Catalyst 9105AX AP introduces latency when clients use RLAN ports.

Caveat ID	Description
CSCwb16086	APs crash with kernel panic when PC is at ieee80211_bsscolor_update_bsscolor_list.
CSCwb16708	Cisco Catalyst 9120AX AP experiences MDIO bus failure.
CSCwb18185	Cisco Aironet 3802 AP experiences kernel panic when PC is at __inode_wait_for_writeback.
CSCwb18410	The Transmission Power for channel 36 in Cisco Catalyst 9120 -E domain AP is lower than the other UNII-I channels.
CSCwb19993	Cisco Aironet 2800 or 3800 AP looses config after an upgrade from 8.10.142.0 to 8.10.168.107.
CSCwa23632	Cisco Catalyst 9800-80 Wireless Controller crashes on 17.3.4 ES9 image.
CSCvy10386	Handle WNCD instance and MCC update handling errors while processing export_anchor_req.
CSCvy63924	Controller crashes after using the **show telemetry ietf subscription all** command.
CSCvz45305	Missing fields are observed when the controller sends the access-request.
CSCvz52986	Cisco Catalyst 9800-80 Wireless Controller experiences crash when running Cisco IOS-XE 17.3.4.
CSCvz64802	The controller gets reloaded when memory corruption occurs in WNCD.
CSCvz67166	The controller drops the CAPWAP connections when the WNCD CPU is high.
CSCvz77768	Cisco Aironet 3700 Series AP brings down the radio after encountering DFS event when non-DFS channels are available.
CSCvz78859	Controller experiences an unexpected reload after an invalid access to the internal hash table.
CSCvz89741	Cisco DNA Center devices are not able to scale in university and stadium scenarios when many events are associated to AP radio with maximum clients.
CSCvz94590	High CPU usage occurs in Syslog Trap when the controller is upgraded to Cisco IOS-XE 17.5.1.
CSCvz95745	Controller displays multiple interference devices with the same device type and different Cluster IDs detected by CleanAir.
CSCvz97915	Controller standby reloads with **device-classifier** configuration and **wr mem** command execution parallely.

Caveat ID	Description
CSCwa07257	APs stop authenticating clients using Flex Local Authentication.
CSCwa20681	Dual Band Radio 0 allows only -3 Tx power when the radio operates in 5-GHz.
CSCwa23659	Controller stops accepting APs to join when no response is received from AP after a DTLS Client Hello.
CSCwa26602	Wired printers cannot discover using **flex mdns gateway** as AP does not query for universal._sub._ipp and universal._sub._ipps.
CSCwa27041	Controller experiences unexpected reboot with Network Mobility Services Protocol (NMSP).
CSCwa29446	VTP does not work on the controller when VLAN information is not propogated.
CSCwa30458	High CPU is observed in the controller when **rif_mgr** process is provoked.
CSCwa33929	Wireless clients get stuck in the IP Learn state after rebooting the controller.
CSCwa64326	Controller experiences crash due to memory leak in SNMP process.
CSCwa65724	Standby reloads with low memory and WNCD crash.
CSCwa73179	Clients with the same UDN domain are unable to view SSDP advertisements from different VLANs.
CSCwa73294	HTTP session, SNMP, and show commands stop working in Cisco Catalyst 9800-80 Wireless Controller when dbm process CPU is high at 100%.
CSCwa76898	WLAN stopped broadcasting after a configuration change in the WLAN profile.
CSCwa78384	The controller crashes and reloads when writing an RP core file with **wncd** in the name.
CSCwa82644	Controller performs incorrect available bandwidth calculations for QBSS_AAC with voice CAC, and FlexConnect AP.
CSCwa84611	Cisco Catalyst 9800-80 Wireless Controller crashes intermittently.
CSCvz39796	CPU HOG messages and tracebacks are noticed during RRM noise report process.
CSCvz57744	Memory leak is observed in Cisco IOS-XE 17.7 throttle images that points to dc_add_dot11_profiles.
CSCvz72172	The **snmp trap link-status** command does not persist through a reload when the command is configured on an interface.

Caveat ID	Description
CSCvz97359	Roaming issue is observed when there is a PMKID mismatch in the controller.
CSCwa08842	APs appear in the controller downloading state due to MD5 mismatch while running Cisco IOS-XE 17.3.4.
CSCwa12806	The controller has stale AP entries that stop further AP configuration.
CSCwa16467	Cleanup client entry in Authenticating state when a client is in RUN state in any controller in the network.
CSCwa22212	Controller profiling does not display the device name from DHCP Option 12.
CSCwa23606	Controller does not display the full certificate when TrustPoint is configured for Webadmin or WebAuth.
CSCwa35309	CAPWAP plumb in Standby fails, if WTP record is not available.
CSCwa35350	AP flaps when WNCd to which it maps report high CPU utilization.
CSCwa37701	Output from **show inventory** displays the Standby unit Chassis as Unknown or ASR1000 power supply even though correct PID is used.
CSCwa51748	Cisco Catalyst 9800 Series Wireless Controller reloads unexpectedly and generates a system-report with Cisco IOS-XE 17.7.1 image.
CSCwa52109	Vendor OUI mismatch prints wrong message when receiving an association or a disassociation request.
CSCwa52721	AP does not assign native VLAN when no VLAN IDs are configured in Policy Profile.
CSCwa76445	An SNMP querier cannot pull data for objects in **cLMobilityGroupMembersOperEntry** table.

Resolved Caveats for Cisco IOS XE, Bengaluru, 17.6.2

Caveat ID	Description
CSCvz55484	Wireless client authentications fail as the controller is unable to send RADIUS packets.
CSCvx71141	Cisco Catalyst 9800-80 Wireless Controller crashes due to a CPU HOG in RRM process.
CSCvx81815	Controller does not send server hello packets to AP when enabling DTLS encryption.

Caveat ID	Description
CSCvy52874	Cisco Catalyst 9115 AP reloads unexpectedly after loading the 17.3.3 ES6 image.
CSCvy67650	Controller does not send TCP SYN or ACK for web redirect when banner size is greater than 200 char.
CSCvy73730	Controller may experience a crash in the cpp-ucode process due to a misaligned DTL.
CSCvy73836	C9800-80 controller goes to rommon after multiple failovers due to power cycling.
CSCvy84153	Crash is observed in the controller when the AP location name is greater than 32 character.
CSCvy89508	The primary member displays "standby hot" even though the standby is in recovery mode.
CSCvy90646	Controller drops incoming CAPWAP keepalive for random APs.
CSCvy92854	C9130 AP running 17.5.1 fast-locate records are not sent even when client is connected to the AP.
CSCvy99116	A crash is observed when a wireless client attempts to connect and the connection times out.
CSCvz08303	Controller reloads unexpectedly in dbm process when DBAL batch stops executing.
CSCvz11154	Continuous memory leak with multiple table entries is observed in FMAN database.
CSCvz12751	RA debugs display port 1812 instead of the configured RADSEC port.
CSCvz15015	Cisco Catalyst 9130AX AP loses its WLAN configuration after moving between controllers.
CSCvz28378	Memory leak observed in WNCD process running 17.3.3 of around 200MB per day.
CSCvz45488	Memory leak is observed in EWLC_OPERATIONAL_DB causing dbm crash.
CSCvz45576	Rogue telemetry updates need to be throttled as the controller punts lot of Rogue reports to DNAC.
CSCvz52851	SSO switchover does not re-establish LISP sessions to the CPs.
CSCvz54928	Client gets stuck in IP learn due to stale entry.
CSCvz63742	Controller does not provide cLApAdminStatus info through SNMP when forensic AWIPS is configured.

Caveat ID	Description
CSCvz80697	Controller does not remove old NMSP entries when new probes are received in a different slot.
CSCvz84691	Controller crashes due to WNCD process when learning an IP address for a client.
CSCvv94885	The **show ap cdp neighbours** command displays the name of the switch instead of the domain name.
CSCvy25684	Different data rates are observed in CLI and RF profiles.
CSCvy74904	AP authorization related RADIUS request does not include the calling station ID and NAS port type.
CSCvy76922	Switch stack with Cisco IOS XE 17.3.2a displays high memory alerts.
CSCvz17623	Memory leak is observed in emulated database and AP join.
CSCvz39749	Client Location Probe displays error when probe request parsing fails.
CSCvz60451	Memory leak is observed in C9800-CL due to native telemetry.
CSCvw70285	Cisco Catalyst 9120 APs cannot send acknowledgement over the air during EAP negotiation.
CSCvx99197	Cisco Catalyst 9120 AP reloads unexpectedly after an upgrade to 8.10.158.38 failed to add RFIC image.
CSCvy03953	Kernel panic crash is observed in Cisco Catalyst 9130 AP.
CSCvy10074	Kernal slab memory leaks are observed in Cisco Aironet 3800 AP on flex local switching WLAN.
CSCvy48917	AP sends corrupted association response when client tries to join the WPA3 AES-802.1x or SHA256 WLAN.
CSCvy59897	Cisco Aironet 4800 Series AP in ELM mode detects its own BSSID as rogue.
CSCvy62022	Roaming client stops receiving IP multicast in a new Cisco Aironet 3800 AP.
CSCvy72869	ICAP AP Radio statistics in Cisco Catalyst 9130 or 9117 APs are missing "Total Frame Error Over Air".
CSCvy75868	Cisco Wave 2 APs crash due to kernel panic.
CSCvy79320	Increased Ping loss after two days of reboot.
CSCvy86698	C9120 AP does not send downstream traffic after a voice call with Tx or Rx traffic using TID 6.

Caveat ID	Description
CSCvz05686	Cisco Aironet 2802 or 3802 AP fails to bring up its radios and continuously logs messages.
CSCvz09846	Cisco Catalyst 9130 AP stale clients in the radio driver table causes associations to fail.
CSCvz09942	Cisco Catalyst 9120AXI AP displays kernel panic in Cisco IOS-XE 17.3.4.30.
CSCvz15425	Cisco Aironet 1815w AP experiences kernel panic when upgraded to the latest 8.5.176.0.
CSCvz24841	Retried 802.11r auth packet forwarded to controller causes duplicate auth responses sent to client.
CSCvz25183	COS AP fragmenting CAPWAP discovery packets are unable to join the controller.
CSCvz49187	Cisco Catalyst 9120 Series AP sends packets with QoS TID when WMM is disabled on WLAN.
CSCvz64239	Cisco Aironet 1815 APs experiences crash in Cisco IOS-XE 17.3.4 ES image.
CSCvz66798	C9120 AP FlexConnect drops ARP request from client to gateway after a WLAN change (local to central).
CSCvz69441	Cisco Catalyst 9115 AP experiences crash due to kernel panic PC.
CSCvw76804	Cisco Aironet 3802 AP drops Zebra client traffic intermittently after fast transition roams.
CSCvx01028	COS AP does not accept WPA2-PSK password on WGB with special character but works fine in IOS AP.
CSCvx37663	Cisco Aironet 1832 AP displays /usr/sbin/capwapd: writing to fd 17 failed!: Input/output error.
CSCvx96224	Numerous core dumps are observed in Cisco Aironet 2800 and 3800 APs slot 1 radios.
CSCvy03587	Macbook clients are stuck in IPLEARN_PENDING status.
CSCvy13594	Cisco Catalyst 9130 AP experiences radio firmware crash on Radio 1 multiple times a day.
CSCvy17092	CSA event after Radar detection is missed in the driver.
CSCvy30091	Cisco Catalyst 9120 AP stops transmitting to Macbook after a session re-authentication.
CSCvy33459	C9130 AP sends packets as TID6 with DSCP 0 in CAPWAP header when configured with link-encryption.

Caveat ID	Description
CSCvy41272	FlexConnect mode with 11k enabled does not work as expected.
CSCvy81859	Packet drops are observed at device driver level .
CSCvy91441	Cisco Aironet 2802 AP experiences radio crash.
CSCvy93234	High Channel Utilization issue is seen in AP device 360 but not in ICAP RF Stats Channel Utilization.
CSCvy94725	Cisco Aironet 2800 and 3800 APs experience Kernel Panic Driver crash when PC is at wlRxRingCleanup.
CSCvy95264	Workgroup bridge (WGB) cannot associate when PSK password contains special characters.
CSCvy95842	Connected AP with non-EWC image undergoes factory reset after reload when DHCP option 43 is set.
CSCvz02579	C9130AXI AP cannot connect to the controller after shut or no shut on a C9300-48H switch interface.
CSCvz05501	Cisco Aironet 2800 AP FW crash is observed in Radio 0.
CSCvz06937	Cisco Catalyst 9120 AP FW crash is observed in Radio 1.
CSCvz18980	Opportunistic Key Caching (OKC) is not pushed from the controller to AP when applied in CLI.
CSCvz36463	Cisco Catalyst 9130 AP flashes insufficient power LED when USB is enabled on PoE+ Switch.
CSCvz44787	Cisco Catalyst 9120AXE AP displays incorrect PID and description for Self Identifying Antenna.
CSCvz46914	OEAP GUI username or password is reset to default when "oeap provisioning-ssid" is disabled.
CSCvz54234	Cisco Catalyst 9124 AP does not maintain the assigned site tag even with the applied write tag.
CSCvz55681	Crash is observed in C9120AXI-B APs joined to C9800-CL running Cisco IOS-XE 17.6.1.
CSCvz59574	Cisco Catalyst 9130 AP: Radio operates in channel 128 and published in channel 56.
CSCvz87088	Cisco Catalyst 9120 APs in monitor mode cannot update neighbor-list causing false honeypot alarms.

Resolved Caveats for Cisco IOS XE, Bengaluru, 17.6.1

Caveat ID	Description
CSCvw92754	Mobilityd crash is observed in the controller.
CSCvw92906	ARP queries flood the network due to low value of Basic Service Set (BSS) max idle period.
CSCvw93611	Incorrect accounting stop class attribute is observed while roaming with non-FT clients.
CSCvw94907	Client data rate is displayed incorrectly in the GUI and CLI.
CSCvw95929	Traceback messages (unable to push WLAN to APs after SSO) are observed after deleting or adding the WLANs in a scaled setup.
CSCvx01611	EoGRE: Add support for AAA-override in open mode (MAB).
CSCvx14179	Static IP on non-Cisco WGB does not work; stuck in IP learn.
CSCvx16484	Controller GUI does not display all locations configured in the Wireless setup.
CSCvx17425	Cisco Catalyst 9115 Series APs: Dynamic Frequency Selection (DFS) detection optimization to avoid false DFS detection.
CSCvx21714	Controller unexpectedly reboots due to qfp-ucode crash.
CSCvx24420	Multiple vulnerabilities in frame aggregation and fragmentation implementation of 802.11.
CSCvx24425	Multiple vulnerabilities in frame aggregation and fragmentation implementation of 802.11.
CSCvx24449	Multiple vulnerabilities in frame aggregation and fragmentation implementation of 802.11.
CSCvx27345	Cisco Catalyst 9800-CL Wireless Controller displays neighbor APs as Rogue in 2.4 GHz band.
CSCvx27626	Apple clients fail to pass Extensible Authentication Protocol over LAN (EAPoL) M2 when 802.11r is enabled after a switchover.
CSCvx35811	CentralWeb Authentication (CWA) clients are not moved back to Web Auth after CoA reauthentication is sent when client is in RUN state.
CSCvx37499	Controller reloads with the reason "Critical process wncd fault on rp_0_0 (rc=139)".
CSCvx37875	Transmission power discrepancies observed in Cisco Catalyst 9130AX and 9117AX Series APs.

Caveat ID	Description
CSCvx39497	WNCD process reloads unexpectedly due to traffic distribution statistics.
CSCvx40586	Controller is not sorting the received RFID RSSI from APs before sending the info to the connector.
CSCvx42772	Cisco Aironet 1832 AP reloads unexpectedly due to kernel panic.
CSCvx44040	Cisco Catalyst 9800-40 WNCD utilises 100 percent of CPU due to local Extensible Authentication Protocol (EAP) authentication loop.
CSCvx44757	Controller in Fabric Mode does not support VNID override on web authentication.
CSCvx50299	APs are unreachable in the inventory even though they are joined to the controller.
CSCvx52078	Cisco Aironet 2802 Series Access Point suddenly drops in transmission power level.
CSCvx56223	Cisco Catalyst 9120AX AP stops allowing new associations on any of the configured SSIDs.
CSCvx56259	FlexConnect central-auth 11r client roaming fails after controller is upgraded to 8.10.142.0.
CSCvx59515	Cisco Catalyst 9800-80 Controller crashes due to switch integrated security features (SISF.
CSCvx61201	Clients are getting incorrect AP VLAN IP.
CSCvx65789	Unexpected reload is generating pttcd and pubd cores.
CSCvx72387	CPU usage of WNCD reaches 100% due to WNCD_DB stuck.
CSCvx78215	Controller reloads unexpectedly at DoubleExceptionVector.
CSCvx88383	Application communication failure.
CSCvx98447	AP reloads unexpectedly with a crash file indicating Hostapd.service failed during boot.
CSCvx99417	Cisco Catalyst 9130AX AP connected client is randomly stuck in IP learning state when Basic Service Set (BSS) coloring is enabled.
CSCvy03953	Cisco Catalyst 9130 AP crash kernel panic "Internal error: Oops - SP/PC alignment exception: 8a000000 [#1] SMP" .
CSCvy06837	Static IP address on the AP is not getting changed when static IP failover is disabled or enabled and comes up via DHCP.
CSCvy11981	Controller reloads unexpectedly due to WNCD (AP name length greater and equal to 32 characters).

Caveat ID	Description
CSCvy17995	Device-tracking doesn't change interface as the controller drops ARP request after roam and IP theft.
CSCvy20300	Primary controller in HA frequently ends abnormally.
CSCvy21906	Roaming client delete due to dot1x timer expiry and EAPOL discards message with aa:aa:03:00:00:00.
CSCvy24126	Cisco Catalyst 9105, 9115, or 9120 Series APs display 100% channel utilization.
CSCvy24397	Local mode AP deletes client if there is no response to EAP request within 30 seconds.
CSCvy30606	The sdn-network-infra-iwan key does not update successfully under a network disruption situation.
CSCvy36594	External WebAuth (EWA) ACLs are lost after changing from HTTP or HTTPS server configuration from the GUI.
CSCvy36698	Multiple Vulnerabilities in Frame Aggregation and Fragmentation Implementation of 802.11.
CSCvy77144	Flex local-sw COS-APs are not plumbing preauth ACL for first client connection attempt for CWA and EWA.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see Troubleshooting TechNotes.

Related Documentation

- Information about Cisco IOS XE
- Cisco Validated Design documents
- MIB Locator to locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets

Cisco Wireless Controller

For more information about the Cisco wireless controller, lightweight APs, and mesh APs, see these documents:

- Cisco Wireless Solutions Software Compatibility Matrix
- Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide
- Cisco Catalyst 9800 Series Wireless Controller Command Reference
- Cisco Catalyst 9800 Series Configuration Best Practices
- In-Service Software Upgrade Matrix

- Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers

The installation guide for your controller is available at:

- Hardware Installation Guides

All Cisco Wireless Controller software-related documentation

Detailed Channels and Maximum Power Settings document for Release 17.6 Supported Access Points

Cisco Catalyst 9800 Series Wireless Controller Data Sheets

- *Cisco Catalyst 9800-CL Wireless Controller for Cloud Data Sheet*
- *Cisco Catalyst 9800-80 Wireless Controller Data Sheet*
- *Cisco Catalyst 9800-40 Wireless Controller Data Sheet*
- *Cisco Catalyst 9800-L Wireless Controller Data Sheet*

Cisco Embedded Wireless Controller on Catalyst Access Points

For more information about the Cisco Embedded Wireless Controller on Catalyst Access Points, see:

https://www.cisco.com/c/en/us/support/wireless/embedded-wireless-controller-catalyst-access-points/tsd-products-support-series-home.html

Wireless Product Comparison

- Compare specifications of Cisco wireless APs and controllers
- Wireless LAN Compliance Lookup
- Cisco AireOS to Cisco Catalyst 9800 Wireless Controller Feature Comparison Matrix

Cisco Access Points–Statement of Volatility

The STATEMENT OF VOLATILITY is an engineering document that provides information about the device, the location of its memory components, and the methods for clearing device memory. Refer to the data security policies and practices of your organization and take the necessary steps required to protect your devices or network environment.

The Cisco Aironet and Catalyst AP Statement of Volatility (SoV) documents are available on the Cisco Trust Portal.

You can search by the AP model to view the SoV document.

Cisco Prime Infrastructure

Cisco Prime Infrastructure Documentation

Cisco Connected Mobile Experiences

Cisco Connected Mobile Experiences Documentation

Cisco Catalyst Center

Cisco Catalyst Center Documentation

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021–2024 Cisco Systems, Inc. All rights reserved.